

VERBATIM <sup>1</sup>RECORD OF TRIAL <sup>2</sup>

(and accompanying papers)

of

MANNING, Bradley E.

(Name: Last, First, Middle Initial)

Headquarters and  
Headquarters Company,  
United States Army Garrison  
(Unit/Command Name)[REDACTED]

(Social Security Number)

U.S. Army

(Branch of Service)

PFC/E-3

(Rank)

Fort Myer, VA 22211

(Station or Ship)

By

GENERALCOURT-MARTIAL

Convened by

Commander

(Title of Convening Authority)

UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON

(Unit/Command of Convening Authority)

Tried at

Fort Meade, MD

(Place or Places of Trial)

on

see below

(Date or Dates of Trial)

## Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012, 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012, 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012, 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013, 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013, 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013, 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013, 16 August 2013, and 19-21 August 2013.

<sup>1</sup> Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)

<sup>2</sup> See inside back cover for instructions as to preparation and arrangement.

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS-A)

### Chapter 4

#### CONCLUSION

##### 4-1. CONCLUSION

a. Access to the Intelligence Enterprise is through the DCGS-A. Commanders, at all echelons, focus on achieving precise situational understanding. This places increased emphasis on dynamic updates of the situation to support on-going operations, contingency planning, development of force packages, and knowledge or awareness to the Commander and staff. DCGS-A provides the Commander the linkage to the three Main Ideas of this Handbook: Reduced Risk, Flattened Network, and the Greatest Impact at the Lowest Level. Commanders depend on the ability of the ISR system to surge/focus collection and analysis efforts leading towards increased situational awareness thus **Reducing Risk**. DCGS-A through a **Flattened Network** provides the capability to all Commanders, especially the **Lowest Level**, to drive the intelligence process and to better articulate their PIR. The ISR cycle can focus on these PIR and answers them in less time through DCGS-A's access to NRT information. DCGS-A provides the access to more information, provides improved analytical tools, and leverages communications, which lead to increased knowledge and awareness.

b. DCGS-A, the Army's Intelligence Flagship system, is in the hands of Soldiers today and is relied upon by Commanders to help them in receiving timely, accurate actionable intelligence thus enabling them to meet combat objectives. DCGS-A, knowledge based, Commander driven, Intelligence for the Warfighter.

c. This Commander's Handbook for DCGS-A is a living document. It will continue to evolve as the system continues to grow. This particular handbook is an overview of the DCGS-A capabilities it provides primarily to the commander. It does not address any particular version of DCGS-A, rather it address the benefits of employment of DCGS-A as a whole.

d. The proponent of this publication is the U.S. Army Intelligence Center and Fort Huachuca. We welcome your comments and recommended changes at any time. You may email them directly to the proponent at james.harper@us.army.mil or mail them to: Commander, U.S. Army Intelligence Center and Fort Huachuca (ATZS-CDI-S), Fort Huachuca, Arizona 85613-6000.

# **ATTACHMENT C**



UNCLASSIFIED // FOUO  
DEPARTMENT OF DEFENSE  
US FORCES AFGHANISTAN  
KABUL, AFGHANISTAN  
APO AE 09356

USFOR-J2

2 July 2010

MEMORANDUM FOR Deputy Commanding General for Support, USFOR-A

SUBJECT: (U) Advanced Analytical Capability Joint Urgent Operational Need Statement

1. Intelligence analysts in theater do not have the tools required to fully analyze the tremendous amounts of information currently available in theater.
2. The impact of this shortfall is felt in almost every activity that intelligence supports. Analysts cannot provide their commanders a full understanding of the operational environment. Without the full understanding of the enemy and human terrain, our operations are not as successful as they could be. This shortfall translates into operational opportunities missed and lives lost.
3. The enclosed need statement describes the capabilities required to ensure our analysts have the tools needed to provide the best analysis required for success in our tough COIN operations.
4. Point of contact is Mr. Pat McNiece, J2 Collection and Requirements, DSN 237-9535, SIPR email: [patrick.b.mcniece@afghan.swa.army.smil.mil](mailto:patrick.b.mcniece@afghan.swa.army.smil.mil).

  
MICHAEL T. FLYNN  
MG, USA  
Deputy Chief of Staff, Intelligence

Enclosure

UNCLASSIFIED // FOUO



UNCLASSIFIED

**JOINT URGENT OPERATIONAL NEED (JUON) REQUEST**

**(U) Title:** USFOR-A Request for Advanced Analytical Capability in Afghanistan (U)

**(U) Reference:**

**(U) Submitted by:** USFOR-A J2 Collection and Requirements

**(U) Date Certified/Prioritized by Combatant Commander:**

**(U) Relative Priority:**

**(U//FOUO) General Description:** US intelligence analysts in Afghanistan have several tools available to access the ever-increasing amount of intelligence and battlefield information residing in a myriad of databases. These tools provide access to the information, some more readily than others, but provide little in the way of improved analytical support. Advanced analytical tools are critical for providing the required intelligence support to population-centric operations.

Current tools do not provide intuitive capabilities to see the relationships between a wide variety of disparate sets of information. They do not allow easy viewing of the information in multiple formats such as link diagram, geo-spatial, histogram, timeline, time wheel and data reports. They do not provide significant network-wide collaborative capabilities. They do not provide the ability to support low-bandwidth or frequently disconnected users with a data sub-set tailored to their area of operations.

There is a critical need to enable analysts in theater with these capabilities to provide our commanders a better understanding of the complex COIN environment in which they operate. Solving these data manipulation, visualization and understanding requirements will significantly improve our ability to successfully conduct population-centric operations.

**(U//FOUO) Mission and Threat Analysis:** Counterinsurgency operations are among the most complex, especially in the Afghan environment. USFOR-A has been challenged in this environment to fully understand the multi-faceted situation. The enemy is able to take advantage of his ability to hide in plain sight in the population because we have been unable to fully exploit the information/intelligence we already have. Detainees with existing connections to the insurgency have been released because we could not fully understand or exploit the information we held. Negative influencers are able to continue hindering progress because we are unable to fully understand their methods and connections. Conversely, we don't know how many opportunities to positively influence events have been lost due to our failure to maximize our understanding of the environment.

UNCLASSIFIED

## UNCLASSIFIED

**(U//FOUO) Structuring and Organization of Capabilities:** This JUON is a request for a theater-wide web-based advanced analytical platform to store, organize, access, retrieve and enable full understanding of intelligence and information from multiple large disparate data sets. We require this capability on three networks: a small capability on JWICS and larger-scale installations for SIPR and the CENTRIXS-ISA Network (CXI). The SIPR network should support SIPR REL for ACGU users. The capability should provide a client-server architecture wherein users at headquarters or high-bandwidth locations access a regional server using their existing workstation. Low-bandwidth or frequently disconnected users should be provided a laptop capable of maintaining the data and applications.

### **(U//FOUO) Critical Performance Specifications:**

- (High Priority) The system will interface with and allow rapid access to existing intelligence and information databases such as CIDNE, DCGS-A, BATS, M3, TIGR, Theater Exploitation Database (TED) and a wide variety of other data sources.
- (High Priority) The system will provide intuitive capabilities to see the relationships between and interact with a wide variety of disparate sets of information in multiple different and flexible views. Specifically the system will provide the following integrated functionalities:
  - The ability to query multiple data sets (held centrally or imported locally via database or spreadsheet)
  - The ability to easily view and manipulate this information in multiple formats (per below) simultaneously or to easily switch between them with one button click to facilitate/improve understanding
  - The ability to create / update / view link diagrams inside different viewing environments such as browser, word documents, map display or the link diagram itself (without onerous detailed entries such as Analyst Notebook)
  - The ability to automatically create a variety of histogram views based on existing data elements (for example, CIDNE IED data auto-creates histograms for IED type, province, district, target, etc.)
  - The ability to show data in a scalable geospatial view, with multiple map/imagery background selections, to quickly create density maps and to be able to query, select and filter data from this view
  - The ability to show data in timeline view, scalable to period desired and to be able to select and filter data from this view
  - The ability to show data in time wheel view with multiple selections for the categories mapped on axis and radius
  - The ability to show data in normal browser/reports view and to select and filter data from this view
- (High Priority) The system will provide significant collaborative capabilities such as ability to share data and results network-wide.
  - This includes the ability to easily publish final results/products or share works in progress with other users

UNCLASSIFIED

## UNCLASSIFIED

- The shared information will include not just the product, but the entirety of the data and queries used, views of the maps, link diagrams, histograms, etc.
- The system should have quick and integrated export to PowerPoint, jpg, html Analyst Notebook and other publishing formats.
- (High Priority) The system will provide the ability to support low-bandwidth or frequently disconnected users with a data sub-set tailored to their area of operations and the applications to use it, as well as the capability to report and update information when re-connected to the network.
  - Users at/near the tactical edge who have only part-time connectivity should be able to use all the above applications on their own specific sub-set of data based on their assigned battle space, even when disconnected.
  - This data set should update while the user is connected to the network and should also feed user reports/work back to the central database for wider use.

**(U/FOUO) Non-Material Alternatives:** There are no known non-material options or alternatives that could meet this capability requirement.

**(U/FOUO) Potential Material Alternatives:** None identified.

**(U/FOUO) Potential Resource Tradeoffs:** None identified.

**(U/FOUO) Constraints:** None identified.

**(U/FOUO) Point of Contact (POC):** USFOR-A/ISAF J2 Collection and Requirements, Mr. Pat McNiece, DSN 318-237-9535, SVOIP 308-237-1584, SIPR email: [patrick.b.mcniece@afghan.swa.army.smil.mil](mailto:patrick.b.mcniece@afghan.swa.army.smil.mil).

**(U/FOUO) Authorized by:** MG Flynn, ISAF/USFOR-A J2.

UNCLASSIFIED

UNCLASSIFIED

**Requirement / Architecture Summary**

1. CXI Network. Combination of regional and, where needed, brigade servers and mobile users. Detailed estimate provided in attached spreadsheet. Summary includes:

- a. Approximately 29 servers supporting almost 4,500 users.
  - b. Approximately 1,750 mobile devices.
- Spreadsheet notes US vs Coalition requirements.

2. SIPR Network. Combination of regional and, where needed, brigade servers and mobile users. Summary includes:

- a. Approximately 18 servers supporting almost 3,000 users.
  - b. Approximately 625 mobile devices.
- Spreadsheet notes US vs 5-Eye Coalition requirements.

3. JWICS Network. Server-client only. Regional servers at the following locations:

- a. Kabul to service JIOC-A, IJC, CFSOCC-A, SOF, NTM-A/CSTC-A (approximately 100 users).
  - b. Bagram to service CJTF-101, SOTF, CJSOTF-A, BCTs (approximately 100 users).
  - c. Kandahar to service KIFC, KFC and BCTs (approximately 100 users).
  - d. Other JWICS users in theater will access one of these servers.
- Summary: 3 server locations servicing approximately 300 users.

UNCLASSIFIED

# **ATTACHMENT D**

**Congress of the United States**  
**Washington, DC 20515**

July 19, 2010

The Honorable Norm Dicks  
Chairman  
House Appropriations Committee  
Subcommittee on Defense  
H-405, The Capitol  
Washington, D.C. 20515

The Honorable C.W. "Bill" Young  
Ranking Member  
House Appropriations Committee  
Subcommittee on Defense  
1016 Longworth House Office Building  
Washington, D.C. 20515

Dear Chairman Dicks and Dear Ranking Member Young:

Please accept this letter regarding a critical intelligence capability known as Global Knowledge Management (GKM) that is urgently needed by our forward deployed forces in Afghanistan but for which current funding shortfalls have prevented full fielding of the capability.

We request that you provide the appropriate funds necessary in the Fiscal Year 2011 Defense Appropriations Bill to competitively source and secure the necessary platform sets for all intelligence and special operations units that have urgently requested the system but have not yet received it. We urge that this funding be administered in consultation with the Inter Agency Technical Support Working Group (TSWG) and Combating Terrorism Technical Support Office (CTTSO), which have been following this issue and have developed significant expertise on this particular capability. Above all, we ask that funding be provided for a system that can operate remotely while disconnected from the network since DoD has struggled with the issue of connectivity in the remote locations where our Special Operators (SOF) are fighting.

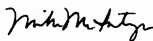
Current fielded systems are incapable of adapting to warfighter conditions in areas of the country that remain underdeveloped. The majority of intelligence collected and archived is not readily available to U.S. forces deployed today. Although significant progress has been made, Commanders remain reliant upon disparate data systems that are not linked automatically, do not work without connectivity and do not seamlessly fuse operational and intelligence information into one picture of the battlespace. As a result, decision making remains time consuming, and significant linkages in patterns of life and cell and network analysis are incomplete, exacerbating a chronic lack of situational awareness, slowing the link between intelligence and action and loosening the kill chain against critical targets.

As you are aware, the fusion of data collection, information management and predictive modeling software tools has been synchronized and packaged into some GKM and discovery platforms that Commanders believe will have a dramatic and positive impact on intelligence gathering and sharing, increasing the operational effectiveness of U.S. and coalition forces. We are told that the GKM network would enable information sharing from far-forward locations in Afghanistan, through theater TOCs, and along a secure NSA-net backbone to the intelligence clearinghouse. This capability can prove to be a game-changer for our teams in theater, but the current level of funding is insufficient to meet the global requirements of our intel teams and SOF elements that have urgently requested them.

Sincerely,



Gabrielle Giffords  
Member of Congress



Mike McIntyre  
Member of Congress



Adam Smith  
Member of Congress

# **ATTACHMENT E**



DEPARTMENT OF THE ARMY  
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-3/5/7  
400 ARMY PENTAGON  
WASHINGTON, DC 20310-0400

July 28, 2010

The Honorable Norm Dicks  
Chairman  
House Appropriations Committee  
Subcommittee on Defense  
H-405, The Capitol  
Washington, DC 20515

Dear Chairman Dicks,

In response to your recent query reference USFOR-A's request for a Global Knowledge Management capability, we understand the specific product in question is the Palantir Technologies analysis tool. In November 2009, the Rapid Equipping Force funded the initial deployment of this tool to support an operational assessment with a deployed Brigade Combat Team (BCT). While this assessment was ongoing, the Intelligence, Surveillance and Reconnaissance Task Force approved and resourced the Army to develop and deploy a Distributed Common Ground Systems - Army (DCGS-A) Cloud Computing environment to Afghanistan in November 2010. This system will provide advanced analysis capability together with storage, web-based access and retrieval functions. The DCGS-A Cloud, together with a software upgrade planned for systems already in theater provides the capabilities required. We will continue to look for opportunities to employ Palantir where the Cloud is not immediately available or where the employed Cloud will not provide adequate coverage. The DCGS-A/Cloud software base is effectively free for CENTCOM as it is already resourced and on track for delivery to theater in response to previously stated CENTCOM requirements.

Sincerely,

A handwritten signature in black ink, appearing to read "PAN", followed by a long horizontal line and a short vertical line at the end.

Peter A. Newell,  
Colonel, US Army  
Director, Rapid Equipping Force



# **ATTACHMENT F**

Congress of the United States

Washington, DC 20515

August 25, 2010

COL Peter A. Newell  
Director - Rapid Equipping Force  
Office of the Deputy Chief of Staff, G-3/5/7  
400 Army Pentagon  
Washington, D.C. 20310-0400

Dear COL Newell:

We recently sent a letter to the Chairman and Ranking Member of the House Defense Appropriations Subcommittee regarding the urgent need for a Global Knowledge Management (GKM) capability that is urgently needed by our forward deployed forces.

According to your letter in response to Chairman Dicks's Inquiry, the Army is planning to field a Cloud computing environment for DCGS-A by this November. While the DCGS-A Cloud Computing environment would be a tremendous advantage over current capabilities for forces deployed to bases with stable and reliable Internet connections, for units deployed to rugged, often uninhabitable terrain - SOF and SF units, specifically - a DCGS-A Cloud-based system will not provide the necessary real time computing capabilities to access necessary data and upload actionable intelligence while on the move. Cloud computing requires an Internet connection to be effective, which may not be available in many areas where the best actionable intelligence is needed or being obtained.

Please provide our staffs with the Rapid Equipping Force's plan to fulfill the need for on-the-move access through the DCGS-A Cloud Computing environment in areas where no reliable Internet connections exist. Secondly, please also provide them with a comprehensive briefing on the status of the DCGS-A development and when you expect it will be deployed to fielded forces.

If you have any questions, please contact our staff directly. We look forward to your prompt reply and appreciate your time and interest. Ryan McKeon is the Senior Legislative Assistant for Military Affairs in the office of Rep. Giffords and can be reached by phone at 202.225.2542 or by email at [ryan.mckeon@mail.house.gov](mailto:ryan.mckeon@mail.house.gov). Brian Garrett is the Military Legislative Assistant for Chairman Smith and can be reached by phone at 202.225.8901 or by email at [brian.garrett@mail.house.gov](mailto:brian.garrett@mail.house.gov).

Sincerely,



Gabrielle Giffords  
Member of Congress



Adam Smith  
Member of Congress

# **ATTACHMENT G**

ADAM SMITH  
9TH DISTRICT, WASHINGTON  
2402 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515  
(202) 225-8901  
COMMITTEE ON ARMED SERVICES  
RANKING MEMBER

DISTRICT OFFICE:  
2209 PACIFIC AVENUE  
SUITE B  
TACOMA, WA 98402  
(253) 593-6600  
TOLL FREE 1-888-SMITH09  
<http://adamsmith.house.gov>  
[http://twitter.com/Rep\\_Adam\\_Smith](http://twitter.com/Rep_Adam_Smith)

**Congress of the United States**  
**House of Representatives**  
**Washington, DC 20515-4709**

May 23, 2011

General Martin E. Dempsey  
Chief of Staff  
United States Army  
1600 Army Pentagon  
Washington, DC 20310-1600

Dear General Dempsey,

One of the reasons for the recent successful mission that resulted in the death of Osama bin Laden was an impressive defense intelligence effort. This success is a reminder of how important analytical capabilities have become in modern warfare and in our fight against global terrorism. It is also a reminder that as much progress as we have made since September 11, 2001, more needs to be done to ensure America's security.

That is why I am concerned that my letter dated August 25, 2010, to the Rapid Equipping Force regarding a Global Knowledge Management (GKM) capability that has gone unacknowledged and without response. For your reference I have attached the original letter and would request your input on this issue.

As you know, on July 2, 2010, Major General Michael Flynn authored a Joint Urgent Operational Needs Statement (JUONS) stating that "intelligence analysts in theater do not have the tools required to fully analyze the tremendous amounts of information currently available in theater." He went on to describe the shortcomings of each tool and indicated that was a far-reaching problem that impacts every analyst in theater.

To date the Army's primary analytical tool has been the Distributed Common Ground Systems (DCGS). I am aware that the Army continues to build its analytical software, as evidenced by a request of \$103 million in research funding in Fiscal Year 2012 in addition to \$103 million in Fiscal Year 2011 funding that was enacted. The House Armed Services Committee has supported past DCGS funding efforts, however, I am troubled that urgent requests for off-the-shelf technologies that meet immediate needs have gone unanswered.

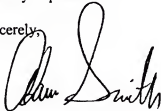
- The JUONS states that current tools "do not provide the ability to support low-bandwidth or frequently disconnected users with a data sub-set tailored to their area of operations." I have been told that the DCGS-A Cloud, the next generation of DCGS-A, meets these requirements. In my letter to the Rapid Equipping Force, I asked that they "provide our staffs with the REF's plan to fulfill the need for...access through the DCGS-A Cloud

Computing environment in areas where no reliable internet connections exist." A cloud requires an always-on internet connection while Afghanistan lacks modern roads much less internet. How does the cloud address this?

- The House Armed Services Committee was told that the Cloud computing environment for DCGS-A would be fielded by this past November. Given the possible shortcoming of the system noted above, has the DCGS-A Cloud been deployed to SOF units in Afghanistan? What kind of reviews has the product received by deployed SOF units? Do off-the-shelf products better meet the needs of SOF units than DCGS-A and if so is there a plan for funding instances of commercially available options, should SOF units actively request them?

I commend the Armed Forces and the intelligence community for their heroic work and the recent successful mission that resulted in the death of Osama bin Laden. In the battle against terror, it was a major success. But further success requires we continue to innovate. We still have an enemy that is capable of plotting against our Homeland and we have men and women in combat who need the best analytic technology to help them succeed. Your prompt response urgently requested.

Sincerely,

A handwritten signature in black ink, appearing to read 'Adam Smith', written over a horizontal line.

Adam Smith  
Member of Congress

# **ATTACHMENT H**

# POLITICO

## Computer bugs hurt Army ops

By Charles Hoskinson  
June 29, 2011 10:33 PM EDT

The Army's \$2.7 billion computing system designed to share real-time intelligence with troops fighting in Afghanistan and Iraq has hurt, rather than helped, efforts to fight insurgents because it doesn't work properly, several analysts who have used the system say.

The analysts' comments mirror concerns raised by the top military intelligence officer in Afghanistan and members of Congress over the past two years in an unsuccessful bid to get the Army to consider alternatives to its portion of the military's Distributed Common Ground System, according to documents obtained by POLITICO.

The Army system, known by the acronym DCGS-A, is a cloud-based computing network designed to collect information from multiple sources for real-time analysis that quickly puts usable intelligence in the hands of battlefield commanders. For example, a commander searching for an insurgent leader would benefit from being able to collect reports of that leader's location and plot them on a map to make tracking easier.

But the analysts say DCGS-A was unable to perform simple analytical tasks. The system's search tool made finding the reports difficult, and the software used to map the information was not compatible with the search software.

"You couldn't share the data," said one former Army intelligence officer who worked in Afghanistan and Iraq.

There were also problems with the hardware, with the system being prone to crashes and frequently going off-line, he and another former Army intelligence officer now working as a contractor in Afghanistan said.

"The laptops are turned on, but it doesn't work," the second former officer said. "There's a lot of bugs in the workflow."

The analysts, who spoke on condition their names not be used, said problems with the DCGS-A system led Maj. Gen. Michael Flynn, the top military intelligence officer in Afghanistan, to write a July 2, 2010, memo citing the urgent need for a new system to analyze the vast amounts of intelligence being collected.

"Analysts cannot provide their commanders a full understanding of the operational environment. Without the full understanding of the enemy and human terrain, our operations are not as successful as they could be," Flynn wrote in the memo obtained by POLITICO. "This shortfall translates into operational opportunities missed and lives lost."

Flynn's memo caught the attention of lawmakers. On July 19, 2010, Democratic Reps. Gabrielle Giffords of Arizona, Mike McIntyre of North Carolina and Adam Smith of Washington wrote to Reps. Norm Dicks (D-Wash.) and Bill Young (R-Fla.), then chairman and ranking Republican on the House Defense Appropriations Subcommittee, seeking urgent funding in fiscal 2011 to "competitively source and secure the necessary platform sets for all intelligence and special operations units that have urgently requested the system but have not yet received it."

The lawmakers, along with several members of the Senate intelligence committee, wanted the Army to consider a rival analytical system produced by Palantir Technologies, a Silicon Valley company founded by PayPal alumni and Stanford computer scientists. Palantir's systems are used by the FBI and the CIA to track suspected terrorists.

Their letters prompted a query from Dicks to the Army. In a response dated July 28, 2010, Col. Peter Newell wrote: "The DCGS-A Cloud, together with a software upgrade planned for systems already in theater, provides the capabilities required. We will continue to look for opportunities to employ Palantir where the Cloud is not immediately available or where the employed Cloud will not provide adequate coverage. The DCGS-A/Cloud software base is effectively free for CENTCOM as it is already resourced and on track for delivery to theater in response to previously stated CENTCOM requirements."

Budget documents, however, show that the Army will have spent more than \$116.7 million on the DCGS-A cloud through the end of September, out of a total program cost of \$1.6 billion over the past four years.

The Army says DCGS-A saves money in two ways: by using mature technology and by eliminating duplication in intelligence, surveillance and reconnaissance systems. "A recent cost-benefit analysis of the DCGS-A program found that this consolidation of ISR systems will result in \$3 billion in cost avoidance over the life of the program," said Army Col. Charles Wells, DCGS-A project manager.

Newell's response to Dicks prompted a written request on Aug. 25, 2010, by Giffords and Smith, now the ranking Democrat on the House Armed Services Committee, for information on how DCGS-A would meet the urgent intelligence needs in Afghanistan identified by Flynn, which went unanswered.

Smith followed up on May 23 with a letter to Army Chief of Staff Gen. Martin Dempsey, implying future funding for the program might be in doubt if lawmakers' concerns aren't addressed. The Army hasn't answered his recent letter either, but an aide to Smith said the Army would respond soon.

"As ranking member of the House Armed Services Committee, it is my primary responsibility to ensure that our troops have the tools and resources necessary to effectively execute their missions. Providing them with timely and useful intelligence — whether at a command post or a forward operating base — is essential to their success," Smith said in a statement. "That is why after the top intelligence officer in Afghanistan



expressed concern regarding the military's ability to analyze information in theater, I asked for additional information surrounding potential shortfalls with the existing approach intended to resolve the issues with the Distributed Common Ground Systems."

"I recently followed up my original request with a subsequent letter and have pushed for a prompt response," Smith added.

Wells said software updates fielded over the past nine months on an expedited basis were intended to support urgent operational needs in Afghanistan.

"The DCGS-A Cloud Node at Bagram, Afghanistan, provides massive storage and processing capabilities that provide unprecedented capabilities for the intelligence analysts in theater," he said. "Through the use of lightweight 'widget' software applications, analysts can query, sort and analyze over 20 million textual intelligence reports in less than one second — allowing them to see subtle connections, associations and patterns that were previously undetectable."

But both former intelligence officers disagreed.

"Almost any commercial solution out there would be better," the first said. And the second added: "It doesn't work. It's not providing the capabilities that they need."

If intelligence analysts and commanders had a system that worked, he said, "I can't comprehend the amount of success that would have happened here or could have happened here."

# **ATTACHMENT I**

# U.S. Army intel software crashes during exercise

By Ben Iannotta  
September 22, 2011

Intelligence software that the U.S. would rely on in a war with North Korea froze up repeatedly during a joint military exercise in South Korea in August, hampering the ability of U.S. and South Korean commanders to watch the movements of simulated enemy forces, a senior intelligence official said.

The Distributed Common Ground System-Army (DCGS-A) software is designed to link intelligence analysts to communications intercepts, imagery and radar collections stored in massive databases. When American intelligence analysts tried to use the software to track simulated North Korean troop movements, the screens on their DCGS-A workstations sometimes went black, forcing them to reboot the software, the senior intelligence official said. Analysts could not always feed the latest enemy positions into the Command Post of the Future, the large computer displays that U.S. commanders would rely on to view troop positions and orchestrate defenses with their South Korean counterparts.

"What happened is the volume of information essentially crashed the software," the senior intelligence official said. "We learned to manually do [data retrieval] in chunks of information so DCGS would not crash." The flaw was discovered during the 10-day Ulchi Freedom Guardian exercise, a computer-generated North Korean attack in which tens of thousands of American and South Korean troops were mobilized in and around Seoul. The Pentagon billed the exercise as a "command post exercise" that would improve coordination of U.S. and South Korean forces.

"Initial analysis indicates that the use of legacy hardware was likely the primary cause of the system reliability issues," a spokesman for the DCGS-A office said in an email. "Personnel running current DCGS-A hardware during the same exercise in Yongin reported no major interruptions, issues, or outages. The issues identified during this exercise are currently being evaluated/corrected as needed."

The Army serves as lead integrator for the version of the software that crashed, incorporating tools and technologies provided by BAE Systems, Northrop Grumman, Overwatch and other contractors. U.S. intelligence officials have lately expressed concern that the wars in Iraq and Afghanistan have honed their ability to untangle insurgent networks and track people, but at the expense of the traditional military intelligence role of tracking forces during high-intensity conflicts involving artillery, tanks and fast-moving troop formations.

This year's Freedom Guardian exercise offered a chance to show that DCGS-A, which is used by analysts and troops in Afghanistan, could perform well in a conventional war.

Software engineers will need to explore whether the greater volume of data stored in the conventional warfare database caused DCGS-A to lock up, the official said.

In a related problem, the DCGS-A system took 2 to 2½ minutes to nominate targets for bombing, a process that should take seconds.

Despite the problems, the senior intelligence official said, the exercise should not be viewed as an indictment of the multibillion-dollar DCGS-A initiative.

"I'm going to make DCGS-A work," the official said.

All told, the DCGS-A system spent 10 out of 96 hours of planned operations locked up or being rebooted, the official said.

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

GOVERNMENT RESPONSE TO  
DEFENSE MOTION FOR  
JUDICIAL NOTICE OF DCGS-A  
INADEQUACIES

17 August 2012

**RELIEF SOUGHT**

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the Defense Motion for Judicial Notice of Distributed Common Ground System-Army (DCGS-A) inadequacies. Specifically, the United States objects to this Court taking judicial notice that the "DCGS-A system was prone to crashes and incapable of functioning when not connected to a network." Def. Mot. at 1.

**BURDEN OF PERSUASION AND BURDEN OF PROOF**

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM), United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2012). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

**FACTS**

1. The United States stipulates to the facts set forth in paragraph 3 of the Defense Motion.
2. The accused was deployed to Iraq from on or about 1 November 2009 to on or about 27 May 2010. *See* Charge Sheet. Attachments C through I to the Defense Motion all post-date the relevant dates of the accused's misconduct. *See* Attachments C through I to the Defense Motion.
3. Attachment C to the Defense Motion, a memorandum from Major General Michael Flynn to the Deputy Commanding General for Support (DCG-S), United States Forces – Afghanistan (USFOR-A), is dated 2 July 2010. *See* Attachment C to the Defense Motion. The memorandum is the cover letter to a Joint Urgent Operational Need (JUON) Statement, requesting a "theater-wide web-based advanced analytical platform to store, organize, access, retrieve and enable full understanding of intelligence and information from multiple large disparate data sets." *Id.* at 3. The theater in question was Afghanistan. *Id.* According to the JUON, the requested system would "interface with and allow rapid access to existing intelligence and information databases, such as CIDNE, DCGS-A, BATS, M3...." *Id.*
4. Attachment E to the Defense Motion, dated 28 July 2010, is a letter from Army Colonel Peter E. Newell to Representative Norm Dicks. *See* Attachment E to the Defense Motion. In the

letter, COL Newell describes the fielding of a DCGS-A Cloud Computing environment to Afghanistan in November 2010. COL Newell states that the DCGS-A Cloud will provide the “capabilities required.” *Id.*

5. Attachment H to the Defense Motion, an article published in “Politico” and dated 29 June 2011, cites two anonymous former Army intelligence officers as saying that the DCGS-A system “was prone to crashes.” See Attachment H to the Defense Motion. At the time of the article, one of the anonymous sources was working as a contractor in Afghanistan. *Id.* The anonymous sources stated that problems with the DCGS-A system led MG Flynn to request a new system in his memorandum dated 2 July 2010. *Id.*

6. Attachment I to the Defense Motion, dated 22 September 2011, describes problems with the DCGS-A system during a joint military exercise in South Korea. See Attachment I to the Defense Motion. According to the article, the DCGS-A system spent 10 out of 96 hours “locked up or being rebooted.” *Id.*

### WITNESSES/EVIDENCE

The United States requests this Court consider the referred Charge Sheet in support of its response.

### LEGAL AUTHORITY AND ARGUMENT

The defense requests this Court take judicial notice that the DCGS-A system “prone to crashes and incapable of functioning when not connected to a network.” Def. Mot. at 1. In short, these “facts” are inappropriate for judicial notice in this case. The defense has provided no support for the proposition that these “inadequacies and issues with the DCGS-A” were well-known or even generally known within the military community. See Def. Mot. at 4.

A judicially noticed fact “must be one not subject to reasonable dispute in that it is either (1) generally known universally, locally, or in the area pertinent to the event or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Military Rule of Evidence (MRE) 201(b). Judicial notice of facts serves as a substitute for testimonial, documentary, or real evidence. Stephen A. Saltzburg, et al., *Military Rules of Evidence Manual* § 201.02[1] (7th ed. 2011). Additionally, judicial notice promotes judicial economy because it relieves a proponent from formally proving certain facts that a reasonable person would not dispute. *Id.* The test for whether an adjudicative fact is “generally known universally, locally, or in the area pertinent to the event” is whether the fact is generally known by “well-informed people.” Saltzburg, *Military Rules of Evidence Manual* § 201.02[3].<sup>1</sup>

Although the defense is correct when it notes that it is not the military judge’s knowledge or experience that is controlling under the first category of adjudicative facts, the defense has

---


<sup>1</sup> The defense’s recitation of judicial notice law is problematic. The two cases they cite – *United States v. Brown* and *United States v. Spann* – do not, in any conceivable way, buttress the propositions for which they are offered. See Def. Mot. at 3.

failed to adequately demonstrate that the DCGS-A inadequacies it articulates are generally known by well-informed people in the military community. Specifically, the defense wants this Court to take judicial notice of the fact that DCGS-A was “prone to crashes,” but provides no evidence that that fact is generally known in the military community, beyond a single article from “Politico.” See Attachment H to the Defense Motion (“There were also problems with the hardware, with the system being prone to crashes and frequently going off-line, he and another former Army intelligence officer now working as a contractor in Afghanistan said.”). Aside from the fact that the defense wants this Court to take judicial notice of what amounts to a single anonymous source statement from an article in “Politico,” the article itself does not mesh with the more reliable evidence provided in Attachment C to the Defense Motion, the memorandum signed by MG Flynn. Attachment H (the “Politico” article) indicates that problems with DCGS-A led MG Flynn to write the 2 July 2010 memorandum (Attachment C) requesting a new system to analyze intelligence; however, the JUON in Attachment C explicitly states that the requested system “will interface with and allow rapid access to existing intelligence and information databases such as CIDNE, DCGS-A, BATS, M3....” See Attachments C and H to the Defense Motion. In short, the JUON in Attachment C says nothing about inadequacies with DCGS-A and in fact states that the requested system would interface with DCGS-A. See Attachment C to the Defense Motion. Thus, it is clear the statements of anonymous sources in the “Politico” article at Attachment H are unreliable and subject to reasonable dispute. Further, it is unclear whether knowledge of DCGS-A inadequacies was widespread, or whether that knowledge was restricted to a small community of anonymous former Army intelligence officers.<sup>2</sup>

Furthermore, the remainder of the attachments to the defense motion are completely unhelpful. For the most part, they consist of correspondence between members of Congress and the Army discussing the need, or lack thereof, for a new intelligence analysis system—the “Global Knowledge Management” capability. The correspondence does not establish, beyond reasonable dispute, that DCGS-A was “prone to crashes and incapable of functioning when not connected to a network.” Aside from the fact that the United States is unclear what is meant by the statement that DCGS-A was “incapable of functioning when not connected to a network,” the defense has provided no reliable evidence of that “fact.”

### CONCLUSION

The United States respectfully requests this Court DENY the Defense Motion for Judicial Notice of DCGS-A inadequacies. For the reasons stated above, the facts sought to be judicially noticed are subject to reasonable dispute in that the Defense has provided no evidence that the “DCGS-A inadequacies” summarized in the Defense Motion were generally known in the military community.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

---

<sup>2</sup> The United States does not concede that the DCGS-A system was an inadequate intelligence tool.

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 17 August 2012.

  
JODEAN MORROW  
CPT, JA

Assistant Trial Counsel

## UNITED STATES

 $\gamma$ 

**MANNING, Bradley E., PFC**

U.S. Army,

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE MOTION FOR  
JUDICIAL NOTICE OF  
EXCERPTS FROM  
DAVID FINKEL'S BOOK  
"THE GOOD SOLDIERS"**

DATED: 3 AUGUST 2012

1. PFC Bradley E. Manning, by and through counsel, moves this court, pursuant to Military Rule of Evidence (M.R.E.) 201 and M.R.E. 801(d)(2)(D) to take judicial notice that David Finkel's book "The Good Soldiers" was published prior to the alleged leaks in this case. The Defense further requests the court take judicial notice that Mr. Finkel's book contains a verbatim transcript of the audio from the video charged in Specification 2 of Charge II.

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting Government property, and two specifications of knowingly exceeding authorized access to a Government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were referred to a general court-martial on 3 February 2012.

APPELLATE EXHIBIT 55  
PAGE REFERENCED: \_\_\_\_\_  
PAGE OF PAGES



5. David Finkel operated as an embedded reporter with 2-16 Battalion, 4th Brigade Combat Team, 1st Infantry Division while the Battalion was deployed to Iraq in 2007. On 12 July 2007, 2-16 conducted operations in the Al-Amin neighborhood of Iraq. As part of this operation, 2-16 employed two AH-64 Apache helicopter gunships. While providing aerial support for the 2-16 operation, members of the Apache crew identified a group of armed men. One minute and fifty five seconds later, after communicating with their command, the crew was given permission to engage the group of men. The crew fired four twenty round bursts over the course of twelve seconds.

6. After the initial burst of gunfire the crew again contacted their command for further permission to engage two individuals who arrived on the scene in a van and were attempting to assist the wounded. Permission was granted and the crew fired upon the van and the individuals assisting the wounded. Two children inside the van were wounded and three more men were killed. Ultimately, the ground reaction force from Bravo Company recovered eleven KIA, including two individuals working as reporters for the Reuters news agency.

7. On 15 September 2009, David Finkel's book, "The Good Soldiers" was published by Farrar, Straus and Giroux. See Attachment B. A portion of the book provides a verbatim account of not only the exchange between the Apache crew and their Headquarters during their engagement with the group, but also the events that happened before, after and contemporaneously. See Attachment A. This 360-degree context clearly indicates that Mr. Finkel was provided a copy of the video in question.<sup>1</sup>

8. On 5 April 2010 the website Wikileaks.org published a video taken from an American Apache helicopter on 12 July 2007. The video depicts the aforementioned engagement and killing of Reuters' employees. The Apache crew audio in the video is identical to the transcript published in Mr. Finkel's book. Moreover, as noted, Mr. Finkel provides additional details about what the Apache crew was seeing at the time, suggesting that he was watching video and listening to audio. For example, Mr. Finkel includes details such as the code words employed by both the Apache crews and 2-16, the exact timing of the conversations relative to the shooting and a vivid description of the battlefield's layout.

#### WITNESSES/EVIDENCE

---

<sup>1</sup> For example, Mr. Finkel details the reaction of the Battalion Commander, then-LTC Ralph Kauzlarich, to the engagement by the Apaches. After the first burst of gunfire, then-LTC Kauzlarich said, "Machine gun fire." Then, after the second burst, he said, "Yeah! We killed more [expletive]." Meanwhile, Mr. Finkel also provides a verbatim account of the Apache crew communications with 2-16. An example of the dialogue:

"All right, you're clear."  
"All right, I'm just trying to find the targets again."  
"We have a bunch of bodies laying there."  
"All right, we got about eight individuals."  
"Yeah, we definitely got some."  
"Yeah, look at those dead bastards."  
"Good shooting."  
"Thank you."

9. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the referenced attachments to this motion in support of its request.

- a. Excerpt from David Finkel's "The Good Soldiers," which also appeared in *The Washington Post* on 6 April 2010.
- b. Amazon.com page for "The Good Soldiers," showing a publication date of 15 September 2009.
- c. MacMillan publishing's biography of David Finkel.

### LEGAL AUTHORITY AND ARGUMENT

10. In the interest of judicial economy, M.R.E. 201 relieves a proponent from formally proving certain facts that reasonable persons would not dispute. There are two categories of adjudicative facts that may be noticed under the rule. First, the military judge may take judicial notice of adjudicative facts that are "generally known universally, locally, or in the area pertinent to the event." M.R.E. 201(b)(1). Under this category of adjudicative facts, it is not the military judge's knowledge or experience that is controlling. Instead, the test is whether the fact is generally known by those that would have a reason to know the adjudicative fact. *U.S. v. Brown*, 33 M.J. 706 (N.M.C.A. 1992). The second category of adjudicative facts are those "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." M.R.E. 201(b)(2). This category of adjudicative facts includes government records, business records, information in almanacs, scientific facts, and well documented reports. *Id.* See also, *U.S. v. Spann*, 24 M.J. 508 (A.F.C.M.R. 1987). The key requirement for judicial notice under this category is that the source relied upon must be reliable.

11. Under M.R.E. 201(d), a military judge must take judicial notice if the proponent presents the necessary supporting information. In making the determination whether a fact is capable of being judicially noticed, the military judge is not bound by the rules of evidence. 1 STEPHEN A. SALTZBURG, LEE D. SCHINASI, AND DAVID A. SCHLUETER, *MILITARY RULES OF EVIDENCE MANUAL* 201.02[3] (2003). Additionally, the information relied upon by the party requesting judicial notice need not be otherwise admissible. *Id.* The determination of whether a fact is capable of being judicially noticed is a preliminary question for the military judge. See M.R.E. 104(a).

12. Here, the excerpt from Mr. Finkel's book is capable of accurate and ready determination by sources that cannot reasonably be questioned. First, Mr. Finkel's is an accomplished author who currently writes for *The Washington Post* and has previously been awarded the Pulitzer Prize for his reporting on U.S. involvement in Yemen. See Attachment C. Moreover, his book was published by Farrar, Straus and Giroux, a major American publishing company. A visit to Amazon.com clearly shows that the book was published on 15 September 2009. Amazon.com is one of the world's largest retailers of books and the accuracy of the publishing information on the site cannot reasonably be questioned. Individuals can purchase the book from any major online book retailer, while those with access to the World Wide Web can read the excerpt by visiting [www.washingtonpost.com](http://www.washingtonpost.com).

13. Mr. Finkel's reputation and the wide-spread availability of the excerpt in question bolster the reliability of the excerpt. The fact that the book offers a verbatim transcript of the events of 12 July 2007, both from the perspective of the Apache crew and members of 2-16, reinforces the fact that Mr. Finkel viewed a copy of the video on question when authoring his book. As such, judicial notice of the excerpt is appropriate in this case.

#### CONCLUSION

14. Based on the above, the Defense requests that the Court to take judicial notice of requested adjudicate facts.

Respectfully Submitted

A handwritten signature in black ink, appearing to read 'Joshua J. Tooman', with a stylized flourish extending to the right.

JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

# **ATTACHMENT A**

# The Washington Post

## U.S. gunfire kills two Reuters employees in Baghdad

By David Finkel  
Washington Post Staff Writer  
Tuesday, April 6, 2010; 12:48 PM

*On July 12, 2007, two employees of the Reuters news agency were killed by gunfire from American helicopters during battle operations in eastern Baghdad, Iraq. A leaked, classified video of those killings was posted yesterday on the web site [Wikileaks.org](http://Wikileaks.org).*

*A fuller account of that day appears in the book "The Good Soldiers," by Washington Post journalist David Finkel, published by Sarah Crichton Books/Farrar, Straus and Giroux. The book chronicles the experiences of the Army's 2-16 Infantry Battalion, commanded by Lieutenant Colonel Ralph Kauzlarich, during "the surge."*

*Finkel was present during the July 12 operation and wrote about that day in the following excerpt.*

On July 12, Kauzlarich ate a Pop-Tart at 4:55 a.m., guzzled a can of Rip It Energy Fuel, belched loudly, and announced to his soldiers, "All right, boys. It's time to get some." On a day when in Washington, D.C., President Bush would be talking about "helping the Iraqis take back their neighborhoods from the extremists," Kauzlarich was about to do exactly that.

The neighborhood was Al-Amin, where a group of insurgents had been setting off a lot of IEDs, most recently targeting Alpha Company soldiers as they tried to get from their COP to Rustamiyah for Crow's memorial service a few days before. Two IEDs exploded on the soldiers that day, leaving several of them on their hands and knees, alive but stunned with concussions, and now Kauzlarich was about to swarm into that area with 240 soldiers, 65 Humvees, several Bradley Fighting Vehicles, and, on loan to them for a few hours from another battalion, two AH-64 Apache helicopter gunships.

All together, it made for a massive and intimidating convoy that at 5:00 a.m. was lining up to leave Rustamiyah when the radar system picked up something flying through the still-dark sky. "Incoming! Incoming!" came the recorded warning as the alert horn sounded. It was a sound that, by now, after so many such warnings, seemed less scary than melancholy, and the soldiers reacted to it with shrugs. Some standing in the open reflexively hit the dirt. The gunners who were standing up in their turrets dropped down into their slings. But most did nothing, because the bullet had been fired, it was only a matter of time, and if they knew anything by now, it was that whatever happened in the next few seconds was the province of God, or luck, or whatever they believed in, rather than of them.

Really, how else to explain Stevens's split lip? Or what happened to a captain named Al Walsh when a mortar hit outside of his door early one morning as he slept? In came a piece of shrapnel, moving so swiftly that before he could wake up and take cover, it had sliced through his wooden door, sliced through the metal frame of his bed, sliced through a 280-page book called *Learning to Eat Soup with a Knife*, sliced through a 272-page book called *Buddhism Is Not What You Think*, sliced through a 128-

ADVERTISEMENT

Take Team USA  
with you.

page book called On Guerrilla Warfare, sliced through a 360-page book called Tactics of the Crescent Moon, sliced through a 176-page Calvin and Hobbes collection, sliced through the rear of a metal cabinet holding those books, and finally was stopped by a concrete wall. And the only reason that Walsh wasn't sliced was that he happened in that moment to be sleeping on his side rather than on his stomach or back, as he usually did, which meant that the shrapnel passed cleanly through the spot where his head usually rested, missing him by an inch. Dazed, ears ringing, unsure of what had just happened, and spotted with a little blood from being nicked by the exploding metal fragments of the ruined bed frame, he stumbled out to the smoking courtyard and said to another soldier, "Is anything sticking out of my head?" And the answer, thank whatever, was no.

Another example: How else to explain what had happened just the day before, in another mortar attack, when one of the mortars dropped down out of the sky and directly into the open turret of a parked Humvee? After the attack was over, soldiers gathered around the ruined Humvee to marvel--not at the destruction a mortar could cause, but at the odds. How much sky was up there? And how many landing spots were down here? So many possible paths for a mortar to follow, and never mind the fact that every one of them comes down in a particular place--the fact that this one followed the one path that brought it straight down through a turret without even touching the edges, a perfect swish, the impossible shot, made the soldiers realize how foolish they were to think that a mortar couldn't come straight down on them.

Resigned to the next few seconds, then, here they were, lined up at the gate, listening to the horn and the incessant, "Incoming! Incoming!" and waiting for whatever was up there to drop.

One second.

Two seconds.

A boom over there.

One second.

Two seconds.

Another boom, also over there.

And nothing here, not even close, no swish this time, so the gunners stood back up, the soldiers in the dirt dusted themselves off, and the massive convoy headed toward Al-Amin to begin a day that would turn out to feature four distinct versions of war.

Arriving just after sunrise, Charlie Company broke off from the convoy and headed to the west side of Al-Amin. It was a saffya daffya day, and the soldiers found no resistance as they began clearing streets and houses. Birds chirped. A few people smiled. One family was so welcoming that Tyler Andersen, the commander of Charlie Company, ended up standing under a shade tree with a man and his elderly father having a leisurely discussion about the war. The Iraqis asked why the Americans' original invasion force had been only one hundred thousand soldiers. They talked about the difficulties of life with only a few hours of electricity a day, and how much they mistrusted the Iraqi government because of the rampant corruption. The conversation, which lasted half an hour and ended in handshakes, was the longest, most civil one Andersen would have with an Iraqi in the entire war, and it filled him with an unexpected sense of optimism about what he and his company of soldiers were doing. That was the first version of war.

The second occurred in the center of Al-Amin, where Kauzlarich went with Alpha Company.

Here, sporadic gunfire could be heard, and the soldiers clung to walls as they moved toward a small neighborhood mosque. They had been tipped that it might be a hideout for weapons, and they wanted to get inside. The doors were chained shut, however, and even if they hadn't been, American soldiers weren't allowed in mosques without special permission. National Police could go in, but the three dozen NPs who were supposed to be part of this operation had yet to show up. Kauzlarich radioed Qasim. Qasim said they were coming. Nothing to do but wait and wonder about snipers. Some soldiers took refuge in a courtyard where a family's wash was hanging out to dry. Others stayed bobbing and weaving on the street, which was eerily empty except for a woman in black pulling along a small girl, who saw the soldiers and their weapons and burst into tears as she passed by.

Here, finally, came the NPs.

"There are weapons inside," Kauzlarich told the officer in charge, a brigadier general.

"No!" the general exclaimed in shock, and then laughed and led his men toward a house next door to the mosque. Without knocking, they pushed through the front door, went past a wide-eyed man holding a baby sucking his thumb, climbed the steps to the roof, took cover for a few minutes when they heard gunfire, jumped from that roof down onto the slightly lower roof of the mosque, went inside, and emerged a few minutes later with a rocket-propelled grenade launcher, an AK-47, ammunition, and, placed carefully into a bag, a partially assembled IED.

"Wow," Kauzlarich said after all this had been brought down to the street, and for a few moments, defying his own order to always keep moving, he stared at the haul, disgusted.

Weapons in a mosque. As a commander, he needed to understand why an imam might allow this, or even sanction it, because as it said in the field manual on Cummings's desk, which was getting dustier by the day, "Counterinsurgents must understand the environment." Good soldiers understood things. So did good Christians, and Kauzlarich desired to be one of those, too. "For he who avenges murder cares for the helpless," he had read the night before in the One Year Bible. "He does not ignore the cries of those who suffer."

Were these people suffering? Yes. Were they helpless? Yes. Was this their version of crying, then? Was the explanation somewhere in the words of Psalms?

But what about a statement released a few days before by an Iraqi religious leader, which said, in part: "Yes, O Bush, we are the ones who kidnap your soldiers and kill them and burn them. We will continue, God willing, so long as you only know the language of blood and the scattering of remains. Our soldiers love the blood of your soldiers. They compete to chop off their heads. They like the game of burning down their vehicles."

What a freak show this place was. And maybe that was the explanation for the pile of weapons Kauzlarich was looking at, that it deserved no understanding whatsoever.

Weapons in a mosque, including an IED to burn vehicles and kill soldiers.

Unbelievable.

Shadi ghabees. Cooloh khara. Allah ye sheelack.

"Shukran," Kauzlarich said out loud to the general, keeping his other thoughts to himself. He made his way to his Humvee to figure out where to go next and was just settling into his seat when he was startled by a loud burst of gunfire.

"Machine gun fire," he said, wondering who was shooting.

But it wasn't machine gun fire. It was bigger. More thundering. It was coming from above, just to the east, where the AH-64 Apache helicopters were circling, and it was so loud the entire sky seemed to jerk.

Now came a second burst.

"Yeah! We killed more [expletive]," Kauzlarich said.

Now came more bursts.

"Holy [expletive]," Kauzlarich said.

It was the morning's third version of war.

One minute and fifty-five seconds before the first burst, the two crew members in one of the circling Apaches had noticed some men on a street on Al-Amin's eastern edge.

"See all those people standing down there?" one asked.

"Confirmed," said the other crew member. "That open courtyard?"

"Roger," said the first.

Everything the crew members in both Apaches were saying was being recorded. So were their communications with the 2-16. To avoid confusion, anyone talking identified himself with a code word. The crew members in the lead Apache, for example, were Crazy Horse 1-8. The 2-16 person they were communicating with most frequently was Hotel 2-6.

There was a visual recording of what they were seeing as well, and what they were seeing now--one minute and forty seconds before they fired their first burst--were some men walking along the middle of a street, several of whom appeared to be carrying weapons.

All morning long, this part of Al-Amin had been the most hostile. While Tyler Andersen had been under a shade tree in west Al-Amin, and Kauzlarich had dealt with occasional gunfire in the center part, east Al-Amin had been filled with gunfire and some explosions. There had been reports of sniper fire, rooftop chases, and rocket-propelled grenades being fired at Bravo Company, and as the fighting continued, it attracted the attention of Namir Noor-Eldeen, a twenty-two-year-old photographer for the Reuters news agency who lived in Baghdad, and Saeed Chmagh, forty, his driver and assistant.

Some journalists covering the war did so by embedding with the U.S. military. Others worked in the periphery. Noor-Eldeen and Chmagh were among those who worked in the periphery, which meant that the military didn't know they were in Al-Amin. The 2-16 didn't know, and neither did the crews of the Apaches, which were flying high above Al-Amin in a slow, counter-clockwise circle. From that height, the crews could see all of east Al-Amin, but the optics in the lead Apache were now focused tightly on



Noor-Eldeen, who had a camera strung over his right shoulder and was centered in the crosshairs of the Apache's thirty-millimeter automatic cannon.

"Oh yeah," one of the crew members said to the other as he looked at the hanging camera. "That's a weapon."

"Hotel Two-six, this is Crazy Horse One-eight," the other crew member radioed in to the 2-16. "Have individuals with weapons."

They continued to keep the crosshairs on Noor-Eldeen as he walked along the street next to another man, who seemed to be leading him. On the right side of the street were some trash piles. On the left side were buildings. Now the man with Noor-Eldeen guided him by the elbow toward one of the buildings and motioned for him to get down. Chmagh followed, carrying a camera with a long telephoto lens. Behind Chmagh were four other men, one of whom appeared to be holding an AK-47 and one of whom appeared to be holding a rocket-propelled grenade launcher. The crosshairs swung now away from Noor-Eldeen and toward one of those men.

"Yup, he's got one, too," the crew member said. "Hotel Two-six, Crazy Horse One-eight. Have five to six individuals with AK-47s. Request permission to engage."

It was now one minute and four seconds before the first burst.

"Roger that," Hotel 2-6 replied. "We have no personnel east of our position, so you are free to engage. Over."

"All right, we'll be engaging," the other crew member said.

They couldn't engage yet, however, because the Apache's circling had brought it to a point where some buildings now obstructed the view of the men.

"I can't get them now," a crew member said.

Several seconds passed as the lead Apache continued its slow curve around. Now it was almost directly behind the building that Noor-Eldeen had been guided toward, and the crew members could see someone peering around the corner, looking in their direction and lifting something long and dark. This was Noor-Eldeen, raising a camera with a telephoto lens to his eyes.

"He's got an RPG."

"Okay, I got a guy with an RPG."

"I'm gonna fire."

But the building was still in the way.

"Goddamnit."

The Apache needed to circle all the way around, back to an unobstructed view of the street, before the gunner would have a clean shot.

Ten seconds passed as the helicopter continued to curve.

"Once you get on it, just open--"

Almost around now, the crew could see three of the men. Just a little more to go.

Now they could see five of them.

"You're clear."

Not quite. One last tree was in the way.

"All right."

There. Now all of the men could be seen. There were nine of them, including Noor-Eldeen. He was in the middle, and the others were clustered around him, except for Chmagh, who was on his cell phone a few steps away.

"Light 'em all up."

One second before the first burst, Noor-Eldeen glanced up at the Apache.

"Come on--fire."

The others followed his gaze and looked up, too.

The gunner fired.

It was a twenty-round burst that lasted for two seconds.

"Machine gun fire," Kauzlarich said quizzically, a half mile away, as the sky seemed to jerk, and meanwhile, here in east Al-Amin, nine men were suddenly grabbing their bodies as the street blew up around them, seven were now falling to the ground, dead or nearly dead, and two were running away--Chmagh and Noor-Eldeen.

The gunner saw Noor-Eldeen, tracked him in the crosshairs, and fired a second twenty-round burst, and after running perhaps twelve steps, Noor-Eldeen dove into a pile of trash.

"Keep shooting," the other crew member said.

There was a two-second pause, and then came the third burst. The trash all around where Noor-Eldeen lay facedown erupted. A cloud of dirt and dust rose into the air.

"Keep shooting."

There was a one-second pause, and then came the fourth burst. In the cloud, Noor-Eldeen could be seen trying to stand, and then he simply seemed to explode.

All of this took twelve seconds. A total of eighty rounds had been fired. The thirty-millimeter cannon was now silent. The pilot was silent. The gunner was silent. The scene they looked down on was one of

swirling and rising dirt, and now, barely visible as some of the swirling dirt began to thin, they saw a person who was taking cover by crouching against a wall.

It was Chmagh.

He stood and began to run. "I got him," someone said, and now he disappeared inside a fresh explosion of dirt, which rose and mingled with what was already in the air as the Apaches continued circling and the crew members continued to talk.

"All right, you're clear," one said.

"All right, I'm just trying to find targets again," another said.

"We have a bunch of bodies laying there."

"All right, we got about eight individuals."

"Yeah, we definitely got some."

"Yeah, look at those dead bastards."

"Good shooting."

"Thank you."

The smoke was gone now and they could see every thing clearly: the main pile of bodies, some prone, one on haunches, one folded into impossible angles; Noor-Eldeen on top of the trash; Chmagh lying motionless on his left side.

"Bushmaster Seven, Crazy Horse One-eight," they radioed to Bravo Company, whose soldiers were on their way to the site. "Location of bodies Mike Bravo Five-four-five-eight-eight-six-one-seven. They're on a street in front of an open courtyard with a bunch of blue trucks, a bunch of vehicles in a courtyard."

"There's one guy moving down there, but he's wounded," someone now said, looking down, scanning the bodies, focusing on Chmagh.

"This is One-eight," the crew member continued on the radio. "We also have one individual who appears to be wounded. Trying to crawl away."

"Roger. We're gonna move down there," Bravo Company replied.

"Roger. We'll cease fire," the Apache crew responded and continued to watch Chmagh, still alive somehow, who in slow motion seemed to be trying to push himself up. He got partway and collapsed. He tried again, raising himself slightly, but again he went down. He rolled onto his stomach and tried to get up on his knees, but his left leg stayed extended behind him, and when he tried to lift his head, he could get it only a few inches off the ground.

"Do you see a shot?" one of the crew members said.

"Does he have a weapon in his hands?" the other said, aware of the rules governing an engagement.

"No, I haven't seen one yet."

They continued to watch and to circle as Chmagh sank back to the ground.

"Come on, buddy," one of them urged.

"All you gotta do is pick up a weapon," another said.

Now, as had happened earlier, their circling brought them behind some buildings that obstructed their view of the street, and when they were next able to see Chmagh, someone they had glimpsed running up the street was crouching over him, a second man was running toward them, and a Kia passenger van was approaching.

"Bushmaster, Crazy Horse," they radioed in urgently. "We have individuals going to the scene. Looks like possibly picking up bodies and weapons. Break--"

The van stopped next to Chmagh. The driver got out, ran around to the passenger side, and slid open the cargo door.

"Crazy Horse One-eight. Request permission to engage."

Ready to fire, they waited for the required response from Bravo Company as two of the passersby tried to pick up Chmagh, who was facedown on the sidewalk. One man had Chmagh by the legs. The second man was trying to turn him over onto his back. Were they insurgents? Were they people only trying to help?

"Come on! Let us shoot."

Now the second man had hold of Chmagh under his arms.

"Bushmaster, Crazy Horse One-eight," the Apache said again.

But there was still no response as the driver got back in his seat and the two men lifted Chmagh and carried him around the front of the van toward the open door.

"They're taking him."

"Bushmaster, Crazy Horse One-eight."

They had Chmagh at the door now.

"This is Bushmaster Seven. Go ahead."

They were pulling Chmagh to his feet.

"Roger, we have a black bongo truck picking up the bodies. Request permission to engage."

They were pushing Chmagh into the van.

"This is Bushmaster Seven. Roger. Engage."

He was in the van now, the two men were closing the door, and the van was beginning to move forward.

"One-eight, clear."

"Come on!"

A first burst.

"Clear."

A second burst.

"Clear."

A third burst.

"Clear."

Ten seconds. Sixty rounds. The two men outside of the van ran, dove, and rolled against a wall as some of the rounds exploded around them. The van continued forward a few yards, abruptly jerked backward, crashed into the wall near the men, and was now enveloped in smoke.

"I think the van's disabled," a crew member said, but to be sure, now came a fourth burst, a fifth, and a sixth--ten more seconds, sixty more rounds--and that, at last, was the end of the shooting.

Now it was a matter of waiting for Bravo Company's soldiers to arrive on the scene, and here they came, in Humvees and on foot, swarming across a thoroughly ruined landscape. The battlefield was theirs now, from the main pile of bodies, to the trash pile with Noor-Eldeen, to the shot-up houses and buildings, to the van--inside of which, among the bodies, they discovered someone alive.

"Bushmaster Six, Bravo Seven," a Bravo Company soldier called over the radio. "I've got eleven Iraqi KIAs, one small child wounded. Over."

The Apache crews were listening.

"Ah, damn," one of them said.

"We need to evac this child," Bravo Seven continued. "She's got a wound to the belly. Doc can't do anything here. She needs to get evac'd. Over."

"Well, it's their fault for bringing their kids to a battle," a crew member said.

"That's right," the other said, and for a few more minutes they continued to circle and watch.

They saw more Humvees arriving, one of which drove up onto the trash pile, right over the part containing what was left of Noor-Eldeen's body.

"That guy just drove over a body."

"Did he?"

"Yeah."

"Well, they're dead, so--"

They watched a soldier emerge from the van cradling the wounded girl and run with her in his arms to the army vehicle that was going to evacuate her to a hospital.

They watched another soldier emerge from the van a few minutes later cradling a second wounded child, this one a little boy who had been discovered under a body presumed to be his father's, which was draped over the boy, either protectively or because that was how a dead man happened to fall.

And then they flew on to another part of Al-Amin as more and more Bravo Company soldiers arrived, one of whom was Jay March, the soldier who on the battalion's very first day in Iraq had climbed a guard tower, peeked out at all of the trash, and said quietly and nervously, "We ain't ever gonna be able to find an IED in all this ..."

Since then, March had learned how prophetic he was, especially on June 25, when an EFP killed his friend Andre Craig, Jr. Craig's memorial service had been on July 7, and now, five days later, as March saw all of the bodies scattered around, blown open, insides exposed, so gruesome, so grotesque, he felt-- as he would later explain--"happy. It was weird. I was just really very happy. I remember feeling so happy. When I heard they were engaging, when I heard there's thirteen KIA, I was just so happy, because Craig had just died, and it felt like, you know, we got 'em."

As the Apaches peeled off, he and another soldier went through a gate in the wall that the van had crashed into and against which Chmagh had tried to take cover.

There, in the courtyard of a house, hidden from street view, they found two more injured Iraqis, one on top of the other. As March looked closer at the two, who might have been the two who had been lifting Chmagh into the van, who as far as March knew had spent the morning trying to kill American soldiers, he realized that the one on the bottom was dead. But the one on top was still alive, and as March looked eyes with him, the man raised his hands and rubbed his two forefingers together, which March had learned was what Iraqis did when they wanted to signal the word friends.

So March looked at the man and rubbed his two forefingers together, too.

And then dropped his left hand and extended the middle finger of his right hand.

And then said to the other soldier, "Craig's probably just sitting up there drinking beer, going, 'Hah! That's all I needed.'"

And that was the day's third version of war.

As for the fourth version, it occurred late in the day, back on the FOB, after Kauzlarich and the soldiers had finished their work in Al-Amin.

They knew by now about Chmagh and Noor-Eldeen.

They had brought back Noor-Eldeen's cameras and examined the images to see if he was a journalist or

an insurgent.

They had gotten the video and audio recordings from the Apaches and had reviewed them several times.

They had looked at photographs taken by soldiers that showed AK-47s and a rocket-propelled grenade launcher next to the dead Iraqis.

They had reviewed every thing they could about what had prefaced the kill ings in east Al-Amin, in other words--that soldiers were being shot at, that they didn't know journalists were there, that the journalists were in a group of men carrying weapons, that the Apache crew had followed the rules of engagement when it fired at the men with weapons, at the journalists, and at the van with the children inside--and had concluded that everyone had acted appropriately.

Had the journalists?

That would be for others to decide.

As for the men who had tried to help Chmagh, were they insurgents or just people trying to help a wounded man?

They would probably never know.

What they did know: the good soldiers were still the good soldiers, and the time had come for dinner.

"Crow. Payne. Craig. Gajdos. Cajimat," Kauzlarich said on the walk to the DFAC. "Right now? Our guys? They're thinking, 'Those guys didn't die in vain. Not after what we did today.'"

Inside the DFAC, the TVs were tuned to Bush's press conference, which had begun in Washington just a few minutes before.

"Our top priority is to help the Iraqis protect their population," Bush was saying, "so we've launched an offensive in and around Baghdad to go after extremists, to buy more time for Iraqi forces to develop, and to help normal life and civil society take root in communities and neighborhoods throughout the country.

"We're helping enhance the size, capabilities, and effectiveness of the

Iraqi security forces so the Iraqis can take over the defense of their own country," he continued. "We're helping the Iraqis take back their neighborhoods from the extremists..."

This was the fourth version of war.

[View all comments](#) that have been posted about this article.

#### Post a Comment

[View all comments](#) that have been posted about this article.

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this

site. Please review the [full rules](#) governing commentaries and discussions. You are fully responsible for the content that you post.

**Sponsored Links**

**Map Your Flood Risk**

Find Floodplan Maps, Facts, FAQs, Your Flood Risk Profile and More!

**1 Sneaky Linguistic Trick**

The secret of how to learn a foreign language in just 10 days. Read here to find out

**QUAN Stock Winner**

Hot Industry, High-Potential Investment - Buy Shares Now!

[Buy a link here](#)

© 2010 The Washington Post Company



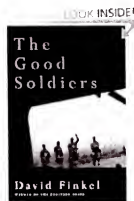
# **ATTACHMENT B**

Your Amazon.com Today's Deals Gift Cards Help

Shop by Department Search **Good Soldiers** Go Hello, Sign In Your Account 0 Cart Wish List

Books Advanced Search Browse Subjects New Releases Best Sellers The New York Times® Best Sellers Children's Books Textbooks Sell Your Books

**The Good Soldiers** and over one million other books are available for Amazon Kindle. [Learn more](#)



## The Good Soldiers [Bargain Price] [Hardcover]

David Finkel (Author)

(147 customer reviews) | (1)

List Price: ~~\$26.00~~

Price: **\$10.40** & eligible for **FREE Super Saver Shipping** on orders over \$25. [Details](#)

You Save: **\$15.60 (60%)**

In Stock.

Ships from and sold by Amazon.com. Gift-wrap available.

**Want it delivered Friday, August 31?** Order it in the next 7 hours and 46 minutes, and choose **One-Day Shipping** at checkout. [Details](#)

**2 new** from \$6.00 **18 used** from \$3.66  
**1 collectible** from \$11.50

**This is a bargain book** and quantities are limited. Bargain books are new but could include a small mark from the publisher and an Amazon.com price sticker identifying them as such. [Details](#)

[Share your own customer images](#)

[Search inside another edition of this book](#)

Start reading *The Good Soldiers* on your Kindle in under a minute.

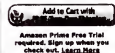
Don't have a Kindle? [Get your Kindle here](#), or download a **FREE Kindle Reading App**.

### Formats

	Amazon Price	New from	Used from
Kindle Edition	—	\$9.99	—
Hardcover, Bargain Price	\$10.40	\$8.00	\$3.66
Paperback	\$10.20	\$4.99	\$0.48
Audio, CD, Audiobook, MP3 Audio, Unabridged	\$12.88	\$8.06	\$8.99
Audible Audio Edition, Unabridged	\$19.95	or Free with Audible	30-day free trial

Quantity: 1

or  
[Sign in](#) to turn on 1-Click ordering.



**Amazon Prime Free Trial** required. Sign up when you check out. [Learn More](#)

**More Buying Choices**

**28 used & new** from \$3.66

Have one to sell?

[Share](#)

## Book Description

Publication Date: **September 15, 2009**

It was the last-chance moment of the war. In January 2007, President George W. Bush announced a new strategy for Iraq. He called it the surge. "Many listening tonight will ask why this effort will succeed when previous operations to secure Baghdad did not. Well, here are the differences," he told a skeptical nation. Among those listening were the young, optimistic army infantry soldiers of the 2-16, the battalion nicknamed the Rangers. About to head to a vicious area of Baghdad, they decided the difference would be them.

Fifteen months later, the soldiers returned home forever changed. Pulitzer Prize-winning *Washington Post* reporter David Finkel was with them in Baghdad, and almost every grueling step of the way.

What was the true story of the surge? And was it really a success? Those are the questions he grapples with in his remarkable report from the front lines. Combining the action of Mark Bowden's *Black Hawk Down* with the literary brio of Tim O'Brien's *The Things They Carried*, *The Good Soldiers* is an unforgettable work of reportage. And in telling the story of these good soldiers, the heroes and the ruined, David Finkel has also produced an eternal tale—not just of the Iraq War, but of all wars, for all time.

## Special Offers and Product Promotions

- Explore more great deals on 1000's of titles in our [Bargain Book store](#).

## Frequently Bought Together

Customers buy this book with WAR by Sebastian Junger **Hardcover \$17.81**



+



**Price For Both: \$28.21**

[Show availability and shipping details](#)

## Customers Who Bought This Item Also Bought

Page 1 of 5



WAR  
 > Sebastian Junger  
 (318)  
 Hardcover  
 \$17.91



The Forever War  
 > Dexter Filkins  
 (164)  
 Paperback  
 \$10.85



The Good Soldiers  
 > David Finkel  
 (147)  
 Paperback  
 \$10.20



They Fought for Each Other:  
 The Triumph and  
 > Kelly Kennedy  
 (28)  
 Hardcover  
 \$10.00



Black Hawk Down: A Story of  
 Modern War  
 > Mark Bowden  
 (713)  
 Paperback  
 \$10.85

## Editorial Reviews

## Amazon.com Review

**Book Description** It was the last-chance moment of the war. In January 2007, President George W. Bush announced a new strategy for Iraq. He called it "the surge." "Many listening tonight will ask why this effort will succeed when previous operations to secure Baghdad did not. Well, here are the differences," he told a skeptical nation. Among those listening were the young, optimistic army infantry soldiers of the 2-16, the battalion nicknamed the Rangers. About to head to a vicious area of Baghdad, they decided the difference would be them.

Fifteen months later, the soldiers returned home forever changed. Pulitzer Prize-winning *Washington Post* reporter David Finkel was with them in Bagdad almost every grueling step of the way.

What was the true story of the surge? Was it really a success? Those are the questions he grapples with in his remarkable report from the front lines. Combining the action of Mark Bowden's *Black Hawk Down* with the literary brio of Tim O'Brien's *The Things They Carried*, *The Good Soldiers* is an unforgettable work of reportage. And in telling the story of these good soldiers, the heroes and the ruined, David Finkel has also produced an eternal tale--not just of the Iraq War, but of all wars, for all time.

## Faces of the Surge

Beneath every policy decision made in the highest echelons of Washington about how a war should be fought are soldiers who live with those decisions every day. These are some of the faces of the U.S. strategy known as "the surge," as photographed by David Finkel, author of *The Good Soldiers*.



Soldiers of the 2-16 Rangers wait for permission to enter a mosque.



Two soldiers try to collect themselves after their Humvee was hit by a roadside bomb.



Sergeant Adam Schumann, regarded as one of the battalion's best soldiers on the day he was sent home with severe post-traumatic stress disorder.

#### From Publishers Weekly

**Starred Review.** A success story in the headlines, the surge in Iraq was an ordeal of hard fighting and anguished trauma for the American soldiers on the ground, according to this riveting war report. *Washington Post* correspondent Finkel chronicles the 15-month deployment of the 2-16 Infantry Battalion in Baghdad during 2007 and 2008, when the chaos in Iraq subsided to a manageable uproar. For the 2-16, waning violence still meant wild firefights, nerve-racking patrols through hostile neighborhoods where every trash pile could hide an IED, and dozens of comrades killed and maimed. At the fraught center of the story is Col. Ralph Kauzlarich, whose dogged can-do optimism—his motto is *It's all good*—pits itself against declining morale and whispers of mutiny. While vivid and moving, Finkel's grunt's-eye view is limited; the soldiers' perspective is one of constant improvisatory reaction to attacks and crises, and we get little sense of exactly how and why the new American counterinsurgency methods calmed the Iraqi maelstrom. Still, Finkel's keen firsthand reportage, its grit and impact only heightened by the literary polish of his prose, gives us one of the best accounts yet of the American experience in Iraq. Photos. (Sept.)

Copyright © Reed Business Information, a division of Reed Elsevier Inc. All rights reserved.

[See all Editorial Reviews](#)

#### Product Details

**Hardcover:** 304 pages

**Publisher:** Farrar, Straus and Giroux; 1 edition (September 15, 2009)

**Language:** English

**ISBN-10:** 0374165734

**ASIN:** B003ZK50U2

**Product Dimensions:** 9.1 x 6.1 x 1.7 inches

**Shipping Weight:** 15.2 ounces ([View shipping rates and policies](#))

**Average Customer Review:** ([147 customer reviews](#))

**Amazon Best Sellers Rank:** #36,547 in Books ([See Top 100 in Books](#))

#29 in [Books > History > Military > Iraq War](#)

#33 in [Books > History > Middle East > Iraq](#)

#62 in [Books > History > Military Science](#)

Would you like to [update product info](#), [give feedback on images](#), or [tell us about a lower price](#)?

#### More About the Author

[Visit Amazon's David Finkel Page](#)

##### Biography

David Finkel is a staff writer for The Washington Post and is also the leader of the Post's national reporting team. He won the Pulitzer Prize for explanatory reporting in 2006 for a series of stories about U.S.-funded democracy efforts in Yemen.

# **ATTACHMENT C**



Search

Advanced Search

BOOKS AUTHORS COMMUNITY

## DAVID FINKEL

Like

Tweet

SIGN UP FOR  
AUTHOR UPDATES

Submit

## MACMILLAN NEWSLETTER

Sign up to receive  
information about new  
books, author events  
and special offers

Sign up now



© Lucien Perkins

**David Finkel** is the author of *The Good Soldiers*, listed a best book of 2009 by the *New York Times*, *Chicago Tribune*, *Slate.com*, and *The Boston Globe*, and winner of the Helen Bernstein Book Award for Excellence in Journalism. He is a staff writer for *The Washington Post*, and is also the leader of the Post's national reporting team. He won the Pulitzer Prize for explanatory reporting in 2006 for a series of stories about U.S.-funded democracy efforts in Yemen. Finkel lives in Silver Spring, Maryland, with his wife and two daughters.

David Finkel

Like

Official Sites

Author Facebook

Related Links



Jump to

Media

Author on the Web

Books by the Author

Community

## MEDIA

Watch

Life in Iraq - David  
Finkel, author of *The  
Good Soldiers*Life in Iraq - David Finkel, author of *The Good Soldiers*

In a video edited by The Washington Post, author David Finkel candidly discusses the uncertainty of life in Iraq

Share This

**MORE MEDIA** Access more related media on this page

[BACK](#)

[David Finkel on GmTV](#)

[David Finkel on The Colbert Report](#)

[David Finkel on Morning Joe](#)

[David Finkel on Charlie Rose](#)

## AUTHOR ON THE WEB

### LATEST ON FACEBOOK



Facebook share page



David Finkel

#### OFFICIAL SITES

[Author Facebook](#)

#### RELATED LINKS



[BACK](#)

## BOOKS BY THE AUTHOR



*The Good Soldiers*

David Finkel  
Picador

A BEST BOOK OF THE YEAR FOR: THE NEW YORK TIMES  
CHICAGO TRIBUNE SLATE.COM THE BOSTON GLOBE THE  
KANSAS CITY STAR THE PLAIN DEALER (CLEVELAND)  
THE

#### AVAILABLE IN



[Buy](#)

BACK

## COMMUNITY

Commandposts.com

## LATEST BLOG POSTS

Wednesday, August 01, 2012 7:54:23 AM

*Glock: Developing the Pistol of the Future*

Monday, July 30, 2012 11:04:34 AM

*The SAS and David Stirling's Leap of Faith*

Friday, July 27, 2012 5:23:09 AM

*Night Over Day Over Night*

## LATEST ON FACEBOOK



Command Posts on Facebook

Like 2,262



Command Posts shared Power Point Ranger's photo.

Congrats to Sergeant Hancock for his successes while competing in the Olympic Games.

Here's to hoping a few days of R&R meet him upon his return home.



Facebook post image

## LATEST ON TWITTER

Join the conversation

BACK

## { ABOUT }

About Macmillan  
 Careers  
 Contact Us

## { SERVICES }

Publishers  
 Booksellers  
 Academic  
 Library  
 Catalogs  
 Macmillan Speakers

## { STORE }

Shopping Cart  
 Your Account  
 Help

## { PUBLISHERS }

Barrow, Straus and Giroux  
 First Second  
 Henry Holt & Co.  
 Macmillan Audio  
 Nature Publishing Group  
 Palgrave Macmillan  
 Plendor  
 Quick and Dirty Tips  
 Scribner American  
 St. Martin's Press  
 Tor/Eureka  
 Unabridged Publishers

## EDUCATION

Macmillan Higher Education  
 Bedford-St. Martin's  
 W. H. Freeman  
 Worth Publishers  
 BFW High School  
 Cengage  
 Hayden-McNeil  
 Palgrave Macmillan  
 Trade Books For Children

## CHILDREN'S

ESQ Books for Young Readers  
 Nature & Friends  
 Math Books for Young Readers  
 Kingfisher  
 Roaring Brook  
 Priddy Books  
 Scholastic  
 Square Fish  
 Young Listeners  
 Macmillan Kids

Privacy Notice Terms of Use Piracy Site Map Visit Our UK Site

© 2011 Macmillan



Appellate Exhibit 235

Enclosure 1

has been entered into  
the record as a CD/DVD  
and will be maintained  
with the original  
Record of Trial

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

GOVERNMENT RESPONSE TO  
DEFENSE MOTION FOR  
JUDICIAL NOTICE OF  
EXCERPTS FROM DAVID FINKEL'S  
BOOK "THE GOOD SOLDIERS"

17 August 2012

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny, in part, the Defense Motion for Judicial Notice of Excerpts from David Finkel's Book "The Good Soldiers." Specifically, the United States objects to the Court taking judicial notice that Finkel's book contains a verbatim transcript of the video charged in Specification 2 of Charge II. The United States does not object to the Court taking judicial notice that Finkel's book was published prior to the leak of the video charged in Specification 2 of Charge II.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM)*, *United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2012). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

The United States stipulates to the facts set forth in paragraphs 3 and 4 of the Defense Motion. Additionally, the United States stipulates to the fact that David Finkel operated as an embedded reporter with 2-16 Battalion, 4th Brigade Combat Team, 1st Infantry Division while the Battalion was deployed to Iraq in 2007. *See* Def. Mot. at 2. The United States also stipulates to the fact that on 5 April 2010, WikiLeaks published a video taken from an American Apache helicopter on 12 July 2007, which depicts an engagement that resulted in the death of two Reuters employees. *Id.*

WITNESSES/EVIDENCE

The United States requests this Court consider the referred Charge Sheet in support of its response.

APPELLATE EXHIBIT 236  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES


## LEGAL AUTHORITY AND ARGUMENT

A judicially noticed fact “must be one not subject to reasonable dispute in that it is either (1) generally known universally, locally, or in the area pertinent to the event or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Military Rule of Evidence (MRE) 201(b). Judicial notice of facts serves as a substitute for testimonial, documentary, or real evidence. Stephen A. Saltzburg, et al., *Military Rules of Evidence Manual* § 201.02[1] (7th ed. 2011). Additionally, judicial notice promotes judicial economy because it relieves a proponent from formally proving certain facts that a reasonable person would not dispute. *Id.*<sup>1</sup>

The defense requests this Court take judicial notice of the fact that “The Good Soldiers” contains a “verbatim transcript of the audio from the video charged in Specification 2 of Charge II.” Def. Mot. at 1. As evidence, the defense provides an excerpt from the book published in *The Washington Post*. See Attachment A to the Defense Motion. While it appears the excerpt describes, in narrative form, parts of the same engagement captured by the video charged in Specification 2 of Charge II, there is no way to determine whether the book excerpt includes a “verbatim” transcript of the video if the defense has not provided the Court with a transcript of the video. In this case, the defense has failed to provide sufficient evidence to allow the Court to make a determination by “resort to sources whose accuracy cannot reasonably be questioned.” MRE 201(b)(2). Accordingly, this Court should deny the defense request to take judicial notice of the fact that “The Good Soldiers” contains a verbatim transcript of the video charged in Specification 2 of Charge II.

## CONCLUSION


The United States respectfully requests this Court DENY, in part, the Defense Motion for Judicial Notice of Excerpts from David Finkel’s Book “The Good Soldiers.” The defense has provided no evidence that “The Good Soldiers” contains a verbatim transcript of the video charged in Specification 2 of Charge II.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

---

<sup>1</sup> The defense’s recitation of judicial notice law is problematic. The two cases they cite – *United States v. Brown* and *United States v. Spann* – do not, in any conceivable way, buttress the propositions for which they are offered. See Def. Mot. at 3.

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 17 August 2012.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

APPELLATE EXHIBIT 22  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_\_ OF \_\_\_\_\_ PAGES

have made the following statements within the scope of their authority and during their employment by the Government:

a. GTMO Documents: "The Wikileaks releases include Detainee Assessment Briefs (DABs) written by the Department of Defense between 2002 and early 2009. These DABs were written based on a range of information available then. The Guantanamo Review Task Force, established in January 2009, considered the DABs during its review of detainee information. In some cases, the Task Force came to the same conclusions as the DABs. In other instances the Review Task Force came to different conclusions, based on updated or other available information. The assessments of the Guantanamo Review Task Force have not been compromised to Wikileaks. Thus, any given DAB illegally obtained and released by Wikileaks may or may not represent the current view of a given detainee." *See Attachment A.*

b. SIGACTS: President Obama "the fact is these documents do not reveal any issues that have not already informed our public debate on Afghanistan.... Indeed, they point to the same challenges that led me to conduct an extensive review of our policy last fall." *See Attachment B.*

Marine Corps Col. David Lapan, a deputy assistant secretary of defense for media operations, told NBC News that a preliminary review by the Pentagon "assessment" team has so far not identified any documents whose release could damage national security. *See Attachment C.*

Former Defense Secretary Robert Gates said in an August 16<sup>th</sup> 2010 letter to the head of the Senate Armed Services Committee that the leak had not revealed any "sensitive intelligence sources or methods." The only real concern noted was the possibility that names of cooperative Afghan nationals may be placed at risk. *See Attachment D.*

Col. Lapan told reporters that a Pentagon team had reviewed the Iraq war files it believes WikiLeaks has, spanning a time period between 2003 and 2010. He described them as largely "ground-level" field reports which could expose the names of Iraqi individuals working with the United States and give insight to Iraqi insurgents about U.S. operations, similar to the Afghan war files. *See Attachment D.*

c. Cables: Secretary Gates' Statement: "Now, I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer, and so on. I think - I think those descriptions are fairly significantly overwrought. The fact is, governments deal with the United States because it's in their interest, not because they like us, not because they trust us, and not because they believe we can keep secrets. Many governments - some governments deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, as has been said before, the indispensable nation. So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another. Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest." *See Attachment E*

Secretary of State Hillary Rodham Clinton at an international security summit reiterated an earlier statement that the leaking of sensitive US diplomatic documents would not hinder

Washington's work with other countries. "I have certainly raised the issue of the leaks in order to assure our colleagues that it will not in any way interfere with American diplomacy or our commitment to continuing important work that is ongoing." She was speaking at a press briefing at the summit of the 56- member Organization for Security and Cooperation in Europe (OSCE) in the Kazakh capital Astana, just days after the documents were released by the whistleblower website WikiLeaks. "I have not had any concerns expressed about whether any nation will not continue to work with and discuss matters of importance ... going forward." See Attachment F

Secretary Clinton has also been quoted on the record saying the leaks merely show, "diplomats doing the work of diplomacy." She further noted, "In a way, it should be reassuring, despite the occasional tidbit that is pulled out and unfortunately blown up. The work of diplomacy is on display, and you know, it was not our intention for it to be released this way -- usually it takes years before such matters are. But I think there's a lot to be said about what it shows about the foreign policy of the United States." See Attachment G

Vice President Biden: "I don't think there's any damage. I don't think there's any substantive damage, no. Look, some of the cables that are coming out here and around the world are embarrassing." See Attachment H.

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman of the Committee on the Judiciary, explained at a hearing before his Committee on 16 December 2010, "[w]e are too quick accept government claims that the risk national security and far too quick to quick to forget the enormous value of some national security leaks." He went on to quote Secretary Gates, "I (Gates) have heard the impact of these releases on our foreign policy described as a meltdown, as a game changer, and so on. I think those descriptions are fairly significantly overwrought." See Attachment I.

#### WITNESSES/EVIDENCE

6. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the referenced attachments to this motion in support of its request.

#### LEGAL AUTHORITY AND ARGUMENT

A. The Statements are Proper for Judicial Notice Under M.R.E. 201

7. In the interest of judicial economy, M.R.E. 201 relieves a proponent from formally proving certain facts that reasonable persons would not dispute. There are two categories of adjudicative facts that may be noticed under the rule. First, the military judge may take judicial notice of adjudicative facts that are "generally known universally, locally, or in the area pertinent to the event." M.R.E. 201(b)(1). Under this category of adjudicative facts, it is not the military judge's knowledge or experience that is controlling. Instead, the test is whether the fact is generally known by those that would have a reason to know the adjudicative fact. *U.S. v. Brown*, 33 M.J.

706, 709 (N.M.C.A. 1992). The second category of adjudicative facts is those “capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” M.R.E. 201(b)(2). This category of adjudicative facts includes government records, business records, information in almanacs, scientific facts, and well documented reports. *Id.* See also, *U.S. v. Spann*, 24 M.J. 508 (A.F.C.M.R. 1987). Moreover, judicial notice may be taken of a periodical. *U.S. v. Needham*, 23 M.J. 383, 385 (C.M.A. 1983) (taking judicial notice of Drug Enforcement Agency publication). The key requirement for judicial notice under this category is that the source relied upon must be reliable.

8. Under M.R.E. 201(d), a military judge must take judicial notice if the proponent presents the necessary supporting information. In making the determination whether a fact is capable of being judicially noticed, the military judge is not bound by the rules of evidence. 1 STEPHEN A. SALTZBURG, LEE D. SCHINASI, AND DAVID A. SCHLUETER, *MILITARY RULES OF EVIDENCE MANUAL* 201.02[3] (2003). Additionally, the information relied upon by the party requesting judicial notice need not be otherwise admissible. *Id.* The determination of whether a fact is capable of being judicially noticed is a preliminary question for the military judge. See M.R.E. 104(a).

9. The Defense requests this court take judicial notice that the statements outlined above were made by the attributed individuals. Here, the statements fall under the second category of facts contemplated by M.R.E. 201(b)(2). Each statement is capable of accurate and ready determination, as each appeared in a mainstream news publication. Indeed, a quick web search for the substance of each quote results in reports from multiple media outlets. Moreover, the accuracy of the sources cannot be reasonably questioned. The statements were made by high-level government officials and were covered by a variety of respected journalistic outlets. Because the statements can be verified by reputable sources, they are the appropriate subject of judicial notice. M.R.E. 201(b)(2)

B. The Statements are Admissible as Non-Hearsay Under M.R.E. 801(b)(2)

10. Any government agency affected by the alleged leaks should be considered a party opponent. *Id.* *U.S. v. American Tel. & Tel. Co.*, 498 F.Supp. 353 (D.C.D.C. 1980) is instructive. At issue were statements made by representatives of various agencies of the Executive Branch at FCC proceedings.<sup>1</sup> The court rejected the government argument that the entire Executive Branch should not be considered a party opponent, noting that the implications of the case extended beyond just the Department of Justice (DOJ). *Id.* at 357. The court also rejected the government’s contention that it should not have to offer explanations for the statements because the government’s size and the varying interests of the numerous government agencies would make offering such an explanation burdensome. The court held:

[T]he underlying theoretical premise of the government’s argument is troubling and cannot be accepted. Its argument in effect is that, whenever the purpose of a rule—whether of pleading or of evidence—would be better effectuated by altering

<sup>1</sup> Specifically at issue was a Brief for the Administrator of General Services, testimony of the Director for Telecommunications Policy, Office of the Secretary of Defense and Proposed Findings of Fact and Argument of the Secretary of Defense. *Id.* at 357.



the configuration of a party to which it is applicable, then the definition of that party must be changed in midstream. Carried to its logical conclusion, this position would force the courts to change the shape and size of parties, particularly in complex litigation, depending upon the part of the case being tried and the principles of law and procedure that may be relevant at any given moment. These chameleon-like shifts in the identity of the parties would upset the orderly conduct of such litigation.

For these reasons, the Court rejects the proposition that the plaintiff in this case for the purposes of the rules of evidence is the Department of Justice; it holds, as it did on September 11, 1978, that the plaintiff is the United States; and it concludes that the statements contained in the three test case documents in question (see note 6 *supra*) constitute admissions by a party-opponent under Rule 801(d)(2). *Id.*

11. Like *American Tel. & Tel. Co.*, this case has far-reaching implications. Indeed, more than just the Departments of the Army and Defense have an interest in the instant case. A number of government agencies, including, but not limited to, the Department of State also had data compromised in the leaks with which PFC Manning is charged. Moreover, the Department of Justice has cooperated extensively in the investigation of the leaks. Further, as the number of damage assessments makes clear, a large number of agencies have reviewed the effect the leaks had on their agency. Presumably, these damage assessments were done because the agency was implicated in some way. Because more than just the Departments of the Army and Defense have been implicated by the leaks at issue in this case, those implicated agencies are also party opponents, *Id.*

12. The statements are admissible under M.R.E. 801(b)(2)(B). M.R.E. 801(b)(2)(B) establishes that "a statement of which the party has manifested the party's adoption or belief in its truth" qualifies as non-hearsay. The court in *U.S. v. Kattar*, 840 F.2d 118, 130 (1st Cir. 1988) addressed this exception. There, the appellant was a member of the Church of Scientology and attempted to introduce statements the government had included in motions for the prosecution of members of the Church of Scientology in an unrelated matter. The court held that DOJ was most certainly a party opponent in a criminal case and the proffer of those statements to a Federal court was an adoption of their truth. Thus, the court held the statements by DOJ were admissible.

13. Here, like in *Kattar*, the parties have adopted the truth of their statements. While these statements were not made as part of court filing, each statement for which judicial notice has been requested was made by a high ranking government official speaking in his/her official capacity. Each statement was made on the record and within the scope of each speaker's government employment and it is fair to assume that the speaker was asserting the content of the statement as the truth. Indeed, any argument by trial counsel to the contrary would serve only to question a high-ranking government official's veracity for truthfulness. Because each speaker has manifested a belief in the truth of his/her statement the statements fall squarely within the non-hearsay contemplated by M.R.E. 801(b)(2)(B).

14. The statements are also admissible pursuant to M.R.E. 801(d)(2)(D). Statements by a party's agent or servant are admissible against that party as long as those statements fall within the agent's or servant's scope of authority and are made while the agency or employment relationship continued. M.R.E. 801(d)(2)(D). Statements made in the scope of employment by a government employee may properly be admitted. *C&H Commercial Contractors v. U.S.*, 35 Fed. Cl. 246, 256 (Fed. Cl. 1996). The court in *U.S. v. Babat*, 18 M.J. 316 (C.M.A. 1984) held, "statements someone makes through an authorized agent are imputable to the principle and may be admitted in evidence against him." *Id.* at 324. The rationale for this rule is that agents or employees have an incentive not to make statements that might damage the party who retains them.

15. While some circuit courts have held that not all statements by government agents should been considered statements by a party opponent under rule 801(d)(2)(D), such holdings are predicated on the idea that an individual cannot bind the sovereign. *U.S. v. Garza*, 448 F.3d 294 (5th Cir. 2006). However, where a government agent is capable of binding the sovereign, statements from that agent are admissible under 801(d)(2)(D). *U.S. v. Salerno*, 937 F.2d 797, 812 (2d. Cir. 1991)(holding that opening and closing statements made by prosecutor in a different, but related criminal prosecution were admissible to show the government once had expressed a different theory about the alleged crime), *see also*, *U.S. v. Johnson*, --- F.Supp.2d ---, 2012 WL 1836282 (N.D. Iowa 2012)(discussing the admissibility of inconsistent factual assertions and inconsistent opinions), *U.S. v. Van Griffin*, 874 F.2d 634, 638 (9th Cir. 1989)(holding that a government manual on field sobriety testing issued by the government was admissible where the agency was a relevant and competent section of the government), *U.S. v. Branham*, 97 F.3d 835, 851 (6th Cir. 1996)(noting that the federal government is a party-opponent of the defendant in a criminal case and a statements by a paid informant were admissible).

16. Here, each of the statements for which judicial notice is requested was made by an individual with the power to bind the sovereign. The statements in questions are not the musings of random Soldiers posted to a blog. Rather, each individual either serves as a high-level government bureaucrat, heading a government agency with the ability to bind the government through policy-making decisions, or, as part of his employment, spoken on behalf of those who did/do have the ability to bind the sovereign. Moreover, these individuals head agencies relevant to this case because each agency was directly affected by the alleged leaks. Because the statements were made by party opponents within the scope of their employment and the party opponents have the ability to bind the sovereign their statements should be deemed admissible under M.R.E. 801(d)(2)(D).

CONCLUSION

17. Based on the above, the Defense requests that the Court to take judicial notice of requested adjudicate facts, and to admit these facts as admissions by a party opponent at trial.

Respectfully Submitted

A handwritten signature in black ink, appearing to read 'Joshua J. Tooman', with a long horizontal flourish extending to the right.

JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

# **ATTACHMENT A**

**The New York Times** Reprints

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers here or use the "Reprints" tool that appears next to any article. Visit [www.nytimes.com](http://www.nytimes.com) for samples and additional information. Order a reprint of this article now.

**BASED ON THE  
TRIUMPHANT  
TRUE STORY**

April 24, 2011

## A Statement by the United States Government

"It is unfortunate that The New York Times and other news organizations have made the decision to publish numerous documents obtained illegally by Wikileaks concerning the Guantanamo detention facility. These documents contain classified information about current and former GTMO detainees, and we strongly condemn the leaking of this sensitive information.

"The Wikileaks releases include Detainee Assessment Briefs (DABs) written by the Department of Defense between 2002 and early 2009. These DABs were written based on a range of information available then.

"The Guantanamo Review Task Force, established in January 2009, considered the DABs during its review of detainee information. In some cases, the Task Force came to the same conclusions as the DABs. In other instances the Review Task Force came to different conclusions, based on updated or other available information. The assessments of the Guantanamo Review Task Force have not been compromised to Wikileaks. Thus, any given DAB illegally obtained and released by Wikileaks may or may not represent the current view of a given detainee.

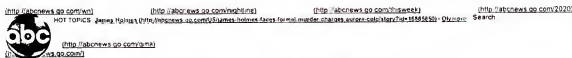
"Both the previous and the current Administrations have made every effort to act with the utmost care and diligence in transferring detainees from Guantanamo. The previous Administration transferred 537 detainees; to date, the current Administration has transferred 67. Both Administrations have made the protection of American citizens the top priority and we are concerned that the disclosure of these documents could be damaging to those efforts. That said, we will continue to work with allies and partners around the world to mitigate threats to the U.S. and other countries and to work toward the ultimate closure of the Guantanamo detention facility, consistent with good security practices and our values as a nation."

**Geoff Morrell****Pentagon Press Secretary**

**Ambassador Dan Fried**

**Special Envoy for Closure of the Guantanamo Detention Facility**

# **ATTACHMENT B**



Home (<http://abcnews.go.com/>) U.S. (<http://abcnews.go.com/us/>) World (<http://abcnews.go.com/international/>)

Politics (<http://abcnews.go.com/politics/>) Videos (<http://abcnews.go.com/video/>) Investigative (<http://abcnews.go.com/investigative/>)

Health (<http://abcnews.go.com/health/>) Entertainment (<http://abcnews.go.com/entertainment/>) Money (<http://abcnews.go.com/business/>)

Tech (<http://abcnews.go.com/technology/>) Travel (<http://abcnews.go.com/travel/>)

## Political Punch (<http://abcnews.go.com/blogs/politics/political-punch/>)

HEADLINES (<http://abcnews.go.com/blogs/headlines/>) POLITICS (<http://abcnews.go.com/blogs/politics/>) ENTERTAINMENT (<http://abcnews.go.com/blogs/entertainment/>)

HEALTH (<http://abcnews.go.com/blogs/health/>) LIFESTYLE (<http://abcnews.go.com/blogs/lifestyle/>) BUSINESS (<http://abcnews.go.com/blogs/business/>)

TECH (<http://abcnews.go.com/blogs/technology/>) TRAVEL (<http://abcnews.go.com/blogs/travel/>)

By Alex Pepper

Jul 27, 2010 1:44pm

## Obama on WikiLeaks: 'Documents Don't Reveal Any Issues that Haven't Already Informed our Public Debate'

ABC News' Yunji de Nies (<http://abcnews.go.com/Politics/story?id=644989&page=1>) and Sunlen Miller (<http://abcnews.go.com/Politics/story?id=704944&page=1>) Report:

President Barack Obama spoke publicly about the WikiLeaks incident for the first time today, expressing concern about the disclosure of tens of thousands of documents, but at the same time, downplaying the content.

"While I'm concerned about the disclosure of sensitive information from the battlefield that could potentially jeopardize individuals or operations, the fact is, these documents don't reveal any issues that haven't already informed our public debate on Afghanistan. Indeed, they point to the same challenges that led me to conduct an extensive review of our policy last fall," Mr. Obama said.

The President reminded reporters in the Rose Garden that that policy review led to a substantial increase in troops and a strategy that he believes can lead to victory.

### About Political Punch

Political coverage and musings on pop culture from ABC News Senior White House Correspondent Jake Tapper and the ABC News White House team.

### ABC News Broadcasts

2010  
(<http://abcnews.go.com/blogs/topics/show>)

GOOD MORNING AMERICA  
(<http://abcnews.go.com/blogs/topics/show-morning-america/>)

NIGHTLINE  
(<http://abcnews.go.com/blogs/topics/show>)

THIS WEEK  
(<http://abcnews.go.com/blogs/topics/show-week/>)

WHAT WOULD YOU DO  
(<http://abcnews.go.com/blogs/topics/show-would-you-do/>)

WORLD NEWS  
(<http://abcnews.go.com/blogs/topics/show-news/>)

WORLD NEWS NOW  
(<http://abcnews.go.com/blogs/topics/show-news-now/>)

WORLD NEWS WITH OJANE SAWYER  
(<http://abcnews.go.com/blogs/topics/show-news-with-ojane-sawyer/>)



"Now we have to see that strategy through. And as I told the leaders, I hope the House will act today to join the Senate, which voted unanimously in favor of this funding, to ensure that our troops have the resources they need and that we're able to do what's necessary for our national security," the President said.

The House is expected to vote today on a war funding bill for the conflicts in Afghanistan and Iraq.

The President spoke after one of a series of regularly scheduled meetings with Congressional leaders from both parties - including House Speaker Nancy Pelosi, Senate Majority Leader Harry Reid, Senate Minority Leader Mitch McConnell, House Minority Leader John Boehner, and House Majority Leader Steny Hoyer.

In addition to the war funding bill, the President said also urged both parties to pass the small business aid bill. The President heads to Edison, NJ tomorrow, where he will hold a roundtable discussion with local business owners, as part of a larger series of trips focused on the economy.

Mr. Obama pledged to keep pushing for broader energy reform including a climate change regulation component, despite last week's setbacks on the Hill with Senate Democrats abandoning climate change legislation.

"The Senate is now poised to act before the August recess, advancing legislation to respond to the BP oil spill and create new clean-energy jobs. That legislation is an important step in the right direction, but I want to emphasize it's only the first step. And I intend to keep pushing for broader reform, including climate legislation."

The President said he also urged Senate Minority Leader Mitch McConnell to allow judicial nominees to be confirmed. Mr. Obama expressed his frustration over a number of nominees who have been voted out of committee, but have not been allowed to begin service because they have yet to have a full vote in the Senate. The President accused "some in the minority" of using "parliamentary procedures time and again" to hold up these nominations.

22 Test |

#### MORE FROM ABC NEWS

['Seinfeld' Star Jumps Into Assault Weapon Debate](http://abcnews.go.com/blogs/politics/2012/07/seinfeld-star-jumps-into-assault-weapon-debate/)  
<http://abcnews.go.com/blogs/politics/2012/07/seinfeld-star-jumps-into-assault-weapon-debate/>

[Limbaugh's 'Dark Knight Rises' Comments 'Bizarro,' Says Nolan](http://abcnews.go.com/blogs/entertainment/2012/07/limbaugh-says-nolan-dark-knight-rises-comments-bizarro/)  
<http://abcnews.go.com/blogs/entertainment/2012/07/limbaugh-says-nolan-dark-knight-rises-comments-bizarro/>

[Governor Welcomes President Obama to Texas By Demanding An Apology](http://abcnews.go.com/blogs/politics/2012/07/governor-welcomes-president-obama-to-texas-by-demanding-an-apology/)  
<http://abcnews.go.com/blogs/politics/2012/07/governor-welcomes-president-obama-to-texas-by-demanding-an-apology/>

[Half of Americans Do Not Know the President's Religion](http://abcnews.go.com/blogs/politics/2012/07/half-of-americans-do-not-know-the-presidents-religion/)  
<http://abcnews.go.com/blogs/politics/2012/07/half-of-americans-do-not-know-the-presidents-religion/>

[Dick Cheney: Picking Sarah Palin for VP Was 'A Mistake'](http://abcnews.go.com/blogs/politics/2012/07/dick-cheneys-picking-serah-palin-for-vp-was-a-mistake/)  
<http://abcnews.go.com/blogs/politics/2012/07/dick-cheneys-picking-serah-palin-for-vp-was-a-mistake/>

[Octomom Asks Fans to Send Money for a New Home](http://abcnews.go.com/blogs/entertainment/2012/07/octomom-wants-to-send-money-for-a-new-home/)  
<http://abcnews.go.com/blogs/entertainment/2012/07/octomom-wants-to-send-money-for-a-new-home/>

# **ATTACHMENT C**

[Subscribe](#) | [Subscription Renewal](#) | [Advertise](#) | [About](#) | [Customer Service](#) | ☐ [RSS](#) | [Digital Edition](#) | [Newsletters](#)

[Log in](#)



<http://www.marinecorpstimes.com/news/2010/10/ap-limited-damage-from-leak-of-afghan-war-logs/>

## Gates: Limited damage from WikiLeaks

By Robert Burns - The Associated Press  
Posted : Friday Oct 15, 2010 16:45:52 EDT

WASHINGTON — No U.S. intelligence sources or practices were compromised by the posting of secret Afghan war logs by the WikiLeaks website, the Pentagon has concluded, but the military thinks the leaks could still cause significant damage to U.S. security interests.

The assessment, outlined in a letter obtained Friday by The Associated Press, suggests that some of the Obama administration's worst fears about the July disclosure of almost 77,000 secret U.S. war reports have so far failed to materialize.

Defense Secretary Robert Gates reported these conclusions in an Aug. 16 letter to Sen. Carl Levin, chairman of the Senate Armed Services Committee, who had requested a Pentagon assessment.

WikiLeaks, a self-described whistle-blower website, is believed to be preparing to release an even larger set of classified Pentagon documents on the Iraq war as early as Sunday.

U.S. officials warned of dire consequences in the days following the July leak. In his letter to Levin, Gates struck a more measured tone in describing the impact.

"Our initial review indicates most of the information contained in these documents relates to tactical military operations," Gates wrote, suggesting the materials did not include the most sensitive kinds of information.

"The initial assessment in no way discounts the risk to national security; however, the review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure," he added.

A Pentagon spokesman, Marine Col. David Lapan, said Friday that the assessment of the July documents is still valid, even after a more thorough review. A special task force led by the Defense Intelligence Agency combed the posted reports for weeks to determine what might have been compromised.

Names of intelligence sources generally are classified at a higher level than the secret-level documents published by WikiLeaks. The documents provided a ground-level view of the war, from 2004 through 2009, based largely on narrow intelligence reports and other battlefield materials.

Gates noted that the documents contained the names of "cooperative Afghan nationals." These were not secret intelligence sources but Afghans who had decided to cut their ties to the Taliban.

The Taliban later vowed to punish these individuals, if the reports proved true.

"We assess this risk as likely to cause significant harm or damage to the national security interests of the United States and are examining mitigation options," Gates wrote. "We are

working closely with our allies to determine what risks our mission partners may face as a result of the disclosure."

So far, the Pentagon has not reported any incidents of reprisals against Afghans named in the leaked documents.

Gates told a news conference on July 29, just a few days after the documents were posted by WikiLeaks, that he had enlisted the help of the FBI to investigate a leak with "potentially dramatic and grievously harmful consequences."

"The battlefield consequences of the release of these documents are potentially severe and dangerous for our troops, our allies and Afghan partners, and may well damage our relationships and reputation in that key part of the world," he said. "Intelligence sources and methods, as well as military tactics, techniques and procedures, will become known to our adversaries."

At the same news conference, Adm. Mike Mullen, chairman of the Joint Chiefs of Staff, said the WikiLeaks operators could face blame for any deadly consequences.

"The truth is, they might already have on their hands the blood of some young soldier or that of an Afghan family," Mullen said.

More recently, U.S. intelligence officials have said the July disclosures sharpened a debate over how far to go in sharing sensitive information within the government, a practice that expanded after Sept. 11, 2001, in order to help prevent future terrorist attacks.

In a speech Oct. 6 to the Bipartisan Policy Center, the director of national intelligence, James Clapper, called the July leaks "a big yellow flag" for those concerned about protecting classified information.

"I think it's going to have a very chilling effect on the need to share," Clapper said.

Military investigators say Army Pfc. Bradley Manning, who served as an intelligence specialist in Baghdad, is a person of interest in the investigation into who provided the Afghan war logs to WikiLeaks.

## Videos You May Be Interested In

### TOP VIDEO PICKS by Taboola



**Decorated war veteran celebr...**  
(2m38s)



**Sailor has Olympic Gold**  
(0m39s)



**Marine dad surprises daug...**  
(1m44s)

### **Insure.com Official Site**

\$250k of Term Life Insurance  
for Under \$1/Day. Free &  
Secure Quotes.  
[LifeInsure.com](http://LifeInsure.com)

### **See New Mortgage Programs**

Mortgages Plunge to 2.5%  
(2.9% APR) FHA Cuts Refi  
Requirement Again!

[AdChoices](#)

**Leave a Comment**

# **ATTACHMENT D**

DON WELLS, ARIZONA  
 JAMES W. WINGTE, OKLAHOMA  
 JEFF SPROWING, ALABAMA  
 F. A. BYE, KANSAS  
 LINDSEY C. GORMAN, SOUTH CAROLINA  
 JOHN T. THOMAS, SOUTH DAKOTA  
 ROGER F. WINKLER, MISSISSIPPI  
 GEORGE L. TERRY, TEXAS  
 BOBBY L. GUNTER, MISSISSIPPI  
 RICHARD W. WHITE, NORTH CAROLINA  
 DON WELLS, ARIZONA  
 F. A. BYE, KANSAS

July 28, 2010

Dear Secretary Gates:

Last Sunday, thousands of classified military documents were published on the internet by an organization called WikiLeaks. Since classified information is, by definition, material that reasonably could be expected to cause damage to the national security if made publicly available, I am concerned about the nature and extent of the damage caused by the release of these documents and the steps that the Department of Defense is taking to address the problem.


Accordingly, I would appreciate your prompt response to the following questions:

1. What is the Department's assessment of the extent to which the documents disclosed on Sunday contain information that was not previously available in the public domain? In the Department's judgment, what are the most significant new disclosures resulting from the release of these documents?
2. What is the Department's assessment of the extent to which sources and methods were divulged as a result of the release of these documents?
3. Has the Department conducted a damage assessment to determine the extent to which individuals may have been put at risk, the enemy may have learned about our tactics and techniques, our allies may be less cooperative in the future, or we may have suffered other specific damage as a result of the release of these documents? If so, what are the conclusions of that assessment?

4. What steps is the Department taking to identify the individual or individuals who released these documents and to prevent future leaks of this kind?

Thank you for your assistance in this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Carl Levin". The signature is fluid and cursive, with the first name "Carl" and last name "Levin" clearly distinguishable.

Carl Levin  
Chairman



1570

SECRETARY OF DEFENSE  
1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000

1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000  
AUG 16 2010

The Honorable Carl Levin  
Chairman  
Committee on Armed Services  
United States Senate  
Washington, DC 20510

Dear Mr. Chairman:

Thank you for your July 28, 2010, letter regarding the unauthorized disclosure and publication of classified military documents by the WikiLeaks organization. I share your concerns about the potential compromise of classified information and its effect on the safety of our troops, allies, and Afghan partners.

After consulting with the Director of the Federal Bureau of Investigation, I have directed a thorough investigation to determine the scope of any unauthorized release of classified information and identify the person or persons responsible. I have also established an interagency Information Review Task Force, led by the Defense Intelligence Agency, to assess the content of any compromised information and the impacts of such a compromise. Our initial review indicates most of the information contained in these documents relates to tactical military operations. The initial assessment in no way discounts the risk to national security; however, the review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure.

The documents do contain the names of cooperative Afghan nationals and the Department takes very seriously the Taliban threats recently discussed in the press. We assess this risk as likely to cause significant harm or damage to the national security interests of the United States and are examining mitigation options. We are working closely with our allies to determine what risks our mission partners may face as a result of the disclosure. There is a possibility that additional military documents may be published by WikiLeaks and the Department is developing courses of action to address this possibility.

The scope of the assessment and nature of the investigative process require a great deal of time and effort. I am committed to investigating this matter and determining

31 JUL 28 2010

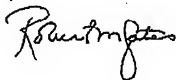


RECEIVED  
SENATE  
SERVICES



appropriate action to reduce the risk of any such compromises in the future. We will keep you informed as additional information becomes available.

Sincerely,

A handwritten signature in dark ink, appearing to read "Robert M. Gates". The signature is fluid and cursive, with the first name "Robert" and last name "Gates" being the most legible parts.

cc:

The Honorable John McCain  
Ranking Member

Home More Bing

Today Daily News Meet the Press Dateline Countdown Madeline HottBall msnbc.com Newsline EveryBody

Search Powerwall



POWERWALL

# PENTAGON PREPS FOR WIKILEAKS RELEASE OF SECRET IRAQ REPORTS

MSNBC Politics, Friday, October 15, 2010, 7:11pm (PDT)

By NBC, msnbc.com and news services

WASHINGTON - The Pentagon is reviewing its war database to prepare for potential fallout from WikiLeaks' expected release of secret documents related to the Iraq war, according to NBC News.

The release could come as early as Sunday evening.

"The problem is we have no idea what WikiLeaks has or is going to release, so we're preparing for the worst," one senior Pentagon official told NBC News on Friday.

WikiLeaks, the controversial online organization set up to reveal government secrets, has indicated it would release as many as 400,000 classified logs from Iraq. In July, WikiLeaks released at least 75,000 U.S. military documents on the Afghan war, including the names of informants and other strategic reports in Afghanistan.

U.S. officials have warned that public revelations about intelligence information can have unpredictable consequences, potentially undermining efforts to monitor and disrupt militant plotting attacks.

Pentagon officials told NBC News they were scouring over 400,000 documents from Iraq they suspect could be what WikiLeaks plans to release next.

Pentagon and military officials say there have been no conversations between WikiLeaks and the Pentagon about reducing highly sensitive or life-threatening information from any classified documents that may be released.

Earlier this year, Pfc. Bradley Manning, an Army intelligence analyst, was charged with providing a classified video to the whistle-blower website.

Manning, 22, is charged with leaking video of a 2007 U.S. Apache helicopter attack in Baghdad that killed a Reuters news photographer and his driver. WikiLeaks posted the video on its website in April.

Military investigators say Manning also is a person of interest in the July leak of the Afghanistan documents.

The Pentagon has concluded that no U.S. intelligence sources or practices were compromised by the posting of secret Afghan war logs by WikiLeaks, but the military thinks the leaks could still cause significant damage to U.S. security interests. The assessment, outlined in a letter obtained Friday by The Associated Press, suggests that some of the Obama administration's worst fears about the July disclosure have so far failed to materialize. Defense Secretary Robert Gates reported these conclusions in an Aug. 16 letter to Sen. Carl Levin, chairman of the Senate Armed Services Committee, who had requested a Pentagon assessment.

U.S. officials warned of dire consequences in the days following the July leak. In his letter to Levin, Gates struck a more measured tone in describing the impact. "Our initial review indicates most of the information contained in these documents relates to tactical military operations," Gates wrote, suggesting the materials did not include the most sensitive kinds of information. "The initial assessment in no way discounts the risk to national security, however, the review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure," he added. A Pentagon spokesman, Marine Col. David Lapan, said Friday that the assessment of the July documents is still valid, even after a more thorough review. A special task force led by the Defense Intelligence Agency combed the posted reports for weeks to determine what might have been compromised. Names of intelligence sources generally are classified at a higher level than the secret-level documents published by WikiLeaks. The documents provided a ground-level view of the war from 2004 through 2009, based largely on narrow intelligence reports and other battlefield materials. Gates noted that the documents contained the names of "cooperative" Afghan nationals. "These were not secret intelligence sources but Afghans who had decided to overthrow the Taliban. The Taliban later vowed to punish these individuals if the reports proved true. "We assess this risk as likely to cause significant harm or damage to the national security interests of the United States and are examining mitigation options," Gates wrote. "We are working closely with our allies to determine what risks our mission partners may face as a result of the disclosure."

Like 0 Tweet 0 more


**Fort Belvoir: Mom Makes \$72Nour Online**  
We investigated how the White LA 200Nour... read full story

**"We Buy Ugly Houses"**  
We Buy Houses in Any Condition... No Agents... Closing Fees... read full story

**E-Cigarette Exposed**  
The E-Cigarette case is sweeping the country... read full story

## MUST READS ON POWERWALL

MOST VIEWED MOST SHARED

### ROYAL SEX LIVES

From secret palace rendezvous to public humiliation, Daily Beast rounds up the Royal sex lives! [READ STORY »](#)


### FLOTUS FASHION

The first lady shows the rest of us how to dress to the nines for any occasion. [VIEW GALLERY »](#)


### FASHIONABLE KATE

Kate Middleton, the Duchess of Cambridge, shows the rest of us how to dress like a modern-day princess. [VIEW GALLERY »](#)


### IS KATE PREGNANT?

Images of a fuller-figured Kate Middleton surface, sparking pregnancy rumors! [READ STORY »](#)


### ROYAL SPORTS

Kate, William and Harry have a sports-filled day together for the first time. [READ STORY »](#)


15 PRICIEST YACHTS

So far, the Pentagon has not reported any sightings of suspected al-Qaeda fighters, armed with leaked documents. More recently, U.S. intelligence officials have said the July disclosures sharpened a debate over how far to go in sharing sensitive information within the government, a practice that expanded after Sept. 11, 2001, in order to help prevent future terrorist attacks. In a speech Oct. 6 to the Bipartisan Policy Center, the director of national intelligence, James Clapper, called the July leaks "a big yellow flag" for those concerned about protecting classified information. "I think it's going to have a very chilling effect on the need to share," Clapper said.



There is arguably no greater symbol of wealth than an enormous, gleaming, luxurious yacht. We take a look at the world's largest.

VIEW GALLERY »

SALLY'S CHOICE

less

## MORE POWERWALL

INSULT TOUR

VP TIMING

### FROM THE WEEK

FROM

FROM

- Mid Romney backs Israel's right to attack
- 10 things you need to know today: July 30
- 10 things you need to know today: July 29
- 10 things you need to know today: July 28
- Jeff Bezos' \$2.5 million gay marriage

- Week in Photos for August 3, 2012
- Roblox Rumor Roundup: Moving Trucks, Tryst
- 'The Last Boys' Where Are They Now?
- Hope Solo Slams Soccer Player Brandi
- Kristen Stewart Cheers on Robert Pattinson

- Holmes charged with murder in Cole shooting
- Pentagon, firm battle over tanks 'we simply
- UNH 200,000 Syrians flee fence fighting in
- Rome's Vatican Colosseum has experts
- Can US men make history in gymnastics final?

NO EASE OVERSEAS

BUBBLE POPPED?

FEMALE PIONEERS

ROYAL DEBUT

LIKING MIT? POVAL SPORTS

SPEAKING UP

BIDEN RESCU TARP INSIDER

THE 'KATE EFFECT'

TOUGH ROAD AHEAD?

SKIPPING

# **ATTACHMENT E**

*The New York Times***The Caucus****The Politics and Government Blog of The Times**

---

NOVEMBER 30, 2010, 7:30 PM

**Gates on Leaks, Wiki and Otherwise***By ELISABETH BUMILLER*

Defense Secretary Robert M. Gates has regularly denounced Wikileaks in recent months for its extensive disclosures, and as a former director of central intelligence he places high value on secrets.

But at a Pentagon briefing on Tuesday, Mr. Gates, who plans to retire next year, responded to a question about Wikileaks' disclosure of 250,000 diplomatic cables by meandering down a different path.

Here is some of what he said:

"Let me just offer some perspective as somebody who's been at this a long time. Every other government in the world knows the United States government leaks like a sieve, and it has for a long time. And I dragged this up the other day when I was looking at some of these prospective releases. And this is a quote from John Adams: 'How can a government go on, publishing all of their negotiations with foreign nations, I know not. To me, it appears as dangerous and pernicious as it is novel.'

"Now, I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer, and so on. I think those descriptions are fairly significantly overwrought. The fact is, governments deal with the United States because it's in their interest, not because they like us, not because they trust us, and not because they believe we can keep secrets. Many governments -- some governments -- deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, as has been said before, the indispensable nation.

"So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another.

"Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest."

# **ATTACHMENT F**

Cars Auto Financing Event Tickets Jobs Real Estate Online Degrees Business Opportunities Shopping

Search

How do I find it?

Subscribe to paper

**ELECTION '12**

**CANDIDATE MATCH GAME 2**  
 Find out which 2012 candidate is your best match

**PLAY NOW!**



Home News Travel Money Sports Life Tech Weather

News » World War casualties

## Clinton: WikiLeaks won't hurt U.S. diplomacy

Updated 12/1/2010 10:10 AM | Comments 40 | Recommend 4

E-mail | Print | RSS



Enlarge

By Deet Vanden Weyngaert, AP

Secretary of State Hillary Rodham Clinton, center, reads a document as she sits next to German Chancellor Angela Merkel at the start of the OSCE Summit at the Palace of Independence in Astana, Kazakhstan on Wednesday.

Kazakhstan details scenes of hard-drinking hedonism by several senior Kazakh ministers. The same report describes Kazakh President Nursultan Nazarbayev as home-obsessed and given to taking refuge from the often-frigid capital at a holiday home in the United Arab Emirates.

Other prospective conference delegates described less than flattering in the leaked cables include Italian Prime Minister Silvio Berlusconi and Russian President Dmitry Medvedev.

"I have certainly raised the issue of the leaks in order to assure our colleagues that it will not in any way interfere with American diplomacy or our commitment to continuing important work that is ongoing," Clinton said. "I have not any had any concerns expressed about whether any nation will not continue to work with and discuss matters of importance to us both going forward."

Several officials at the summit echoed her comments.

British Deputy Prime Minister Nick Clegg, who met Wednesday with Clinton, released a statement saying the "recent WikiLeaks disclosures would not affect our uniquely strong relationship."

Kazakh Foreign Minister Kanat Saudabayev also said "this will have no bearing on our strategic relationship."

The Obama administration has harshly criticized the leaking of the cables, saying the details in them could put lives at risk.

"I anticipate that there will be a lot of questions that people have every right and reason to ask, and we stand ready to dispense that at any time with our counterparts around the world," Clinton added.

On the sidelines of the summit, Clinton and her Belarusian counterpart, Sergei Martynov, announced that the former Soviet republic of Belarus will give up its stockpile of material used to make nuclear weapons by 2012.

That's a significant step forward in efforts aimed at reducing the risk of nuclear materials falling into the hands of terrorists, and follows similar commitments made by other former Soviet republics, including Kazakhstan. Washington will provide technical and financial help to enable Belarus to dispose of its highly enriched uranium stocks.

Clinton said the Obama administration is encouraged that Iran has agreed to return to Geneva for a new round of international talks on its disputed nuclear program. However, a uranium-exchange agreement that was announced following talks with Iran in October 2009 — but which later unraveled — would have to be modified to take into account the fact that Iran has since produced more enriched uranium, she said.

The OSCE was born in the 1970s to nurture rapprochement between Cold War enemies. But the organization has in recent years struggled to define a clear purpose — an anxiety reflected in the speeches of many leaders at the Astana summit. Failure to achieve any breakthrough in Europe's various territorial stalemates, from Moldova's separatist Trans-Dniester region to the perennial tension between Armenia and Azerbaijan over the contested Nagorno-Karabakh region, has served as an embarrassing reminder of the OSCE's weakness to effect significant change.

In a thinly veiled broadcast at Russia, Clinton chided efforts to obstruct the placement of an OSCE mission in Georgia, whose own territorial integrity has been undermined by Moscow's diplomatic and financial support for the breakaway regions of Abkhazia and South Ossetia.

"It is regrettable that a participating state has proposed to host a mission, and the OSCE has not been allowed to respond," Clinton said.

ASTANA, Kazakhstan (AP) — The leak of thousands of sensitive U.S. embassy cables will not hurt American diplomacy, Secretary of State Hillary Rodham Clinton declared Wednesday at a security summit.

Clinton said she has discussed the revelations published on the WikiLeaks website with her colleagues at the summit in Astana, the capital of Kazakhstan. The event is the first major international meeting of leaders and top diplomats since the mamos began appearing on the website and in international publications this week.

The secret memos published by WikiLeaks contain frank details on several leaders attending the Organization for Security and Cooperation in Europe meeting. One note allegedly written by a U.S. diplomat in

Share

Add to Mixx

Facebook

Twitter

More

Subscribe

myYahoo

iGoogle

More

### Videos you may be interested in

McCain defends Clinton aide

Michelle Obama, David Beckham smoke goals

Are Annette's 'Sister' Sisters/Annette's Sister

by Taboo

More videos

**ELECTION '12**

**CANDIDATE MATCH GAME 2**  
 Find out which 2012 candidate is your best match

**PLAY NOW!**

### Most Popular E-mail Newsletter

Sign up to get:



Sign up for USA TODAY E-mail newsletters

Copyright 2010 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Talking Tech with musician James Taylor (USATODAY.com in Tech)  
 'Deeperate Housewife,' 'Selens' actress Lupe Ontiveros dies (USATODAY.com in LifeLine Live)  
 Tweet show: Stewart-Pattinson scandal in 140 characters (USATODAY.com in Life)  
 DA: Mom dad shoots 2 kids, 1 fatally, kills self (USATODAY.com in News)

Selected for you by a sponsor

The Most-Spoiled Children in the U.S. Live In... (Women&Co.)

Figure 8

Posted 12/1/2010 9:55 AM

Updated 12/1/2010 10:10 AM

E-mail | Print |   

To report corrections and clarifications, contact Standards Editor Brent Jones. For publication consideration in the newspaper, send comments to [letters@usatoday.com](mailto:letters@usatoday.com). Include name, phone number, city and state for verification. To view our corrections, go to [corrections.usatoday.com](http://corrections.usatoday.com).

**Guidelines:** You share in the USA TODAY community, so please keep your comments smart and civil. Don't attack other readers personally, and keep your language decent. Use the "Report Abuse" button to make a difference. [Read more](#)

You must be logged in to leave a comment. [Log in](#) | [Register](#)

Post this comment to Facebook?

Comments: (40) Showing Newest first • New Most recommended!

Domalshive7 (3 friends, send message) wrote 12/2/2010 5:45:18 PM

WON'T HURT US Diplomacy??? REALLY?

MAY BE, But I am sure Israeli-Kazakh mining tycoon Alexander Machkevich, worth \$3.3 billion, wants to kick the US Diplomat's ass for back stubbing him after 4 dinner invitations: (read on...)

In a somewhat catty missive, the U.S. diplomat reveals he was unimpressed with Machkevich's parties:

"It is not clear what Mashkova is spending his billions on, but it is certainly not culinary talent. On all four occasions the Ambassador has eaten at one of his houses, the menu has been similar and focused on beefsteak (boiled meat and noodles) and plov. The staff appeared to be graduates of a Soviet cafeteria training academy. The wine, at least, was somewhat upscale with reasonably good French vintage bottles uncorked for the guests. The Astena residence has wooden plaques on the doors that would fit nicely in a Wyoming hunting lodge but are somewhat out of touch with the upscale "Euro-remont" that is so popular among the Kazakhstan elite." (I got this passage of the leak from the Forbes.com website, just in case you are wondering)

SO think this guy will invite another US diplomat to his Parties or even have TRUST in the US Diplomacy?

[Recommend](#) [Report Abuse](#)

Orlando (133 friends) send message wmf. 12/2/2010 2:25:03 PM

There is no US diplomacy. The leaks demonstrate our entire program is based on back door discussions with thugs along with bribes thrown in at every turn. We go around the world with suit cases of money buying up whatever we need.

Recommended 11. Report Abuse



melee401 (127 friends, send message) wrote 12/2/2010 2:09:57 PM

User Image

Greedy Sin (0 friends, send message) wrote, 1d ago

I agree. What is more Hillary is trying to steer public opinion with her out to lunch remarks here. Those emails and memos appeared to have been written by arrogant, self bloating, thoughtless



# **ATTACHMENT G**

# CNN Politics

SEARCH

[Home](#) | [Video](#) | [NewsPulse](#) | [U.S.](#) | [World](#) | [Politics](#) | [Justice](#) | [Entertainment](#) | [Tech](#) | [Health](#) | [Living](#) | [Travel](#) | [Opinion](#) | [iReport](#) | [Money](#) | [Sports](#)

Ads by Google

## Basement Waterproofing

Waterproofing, Foundation Repair & Mold Removal Services. Call Us Now!

[ThompsonsWaterproofing.com](#)

## Support President Obama

Show Your Support for Pres. Obama's Agenda. Add Your Name Here!

[DSCC.org/Support-Obama](#)

### Related Articles »

Clinton reassures leaders amid WikiLeaks disclosure  
December 1, 2010

Clinton condemns leak as 'attack on international community'  
November 29, 2010

WikiLeaks again reports electronic disruption  
November 30, 2010

### Find More Stories About »

Foreign Policy  
WikiLeaks  
Diplomats  
Diplomacy

Advertisement

## FOREIGN POLICY

# Clinton: WikiLeaks cables show diplomacy at work

December 04, 2010 | By the CNN Wire Staff

The confidential U.S. embassy cables posted online by the website WikiLeaks simply show "diplomats doing the work of diplomacy," U.S. Secretary of State Hillary Clinton said Saturday.

Clinton said she was not making light of the leaked documents, which reveal secret communications from U.S. diplomats around the world and have caused embarrassment for the United States and others.

"Everybody is concerned," she told reporters aboard her plane as it departed Bahrain, where she spoke at a conference. "Everybody has a right to have us talk to them, and have any questions that they have answered, but at the end of the day — as a couple of analysts and writers are now writing — what you see are diplomats doing the work of diplomacy."

Ads by Google

## Mitt Romney and Bain

Turning around failing businesses Get the facts about Obama's attacks  
[www.MittRomney.com](#)

## Lilly Ledbetter on Obama:

"He has two daughters, and he wants things better for them." See why.  
[www.barackobama.com/our-vote](#)

Recommend

68 people recommend this. Be the first of your friends.



GETTY IMAGES

Advertisement



The secretary made the comments off-camera but on the record.

Clinton said she has been working hard to re-establish trust and relationships that may have been harmed by the leaks. Many countries had questions that she had to answer, and she has had to reassure them, but she said many also realize U.S. outreach and diplomacy will continue.

"But I haven't seen everybody in the world, and apparently there's 252,000 of these things out there in cyberspace somewhere," she said of the documents, "so I think I'll have some outreach to continue doing over the next weeks just to make sure as things become public, if they raise concerns, I will be prepared to reach out and talk to my counterparts or heads of state or government."

Asked whether President Obama has had to call any heads of state, Clinton said she wasn't sure, though he had made recommendations for calls and would raise the issue as he speaks to counterparts on other matters.

"In a way, it should be reassuring, despite the occasional tidbit that is pulled out and unfortunately blown up," Clinton said. "The work of diplomacy is on display, and you know, it was not our intention for it to be released this way — usually it takes years before such matters are. But I think there's a lot to be said about what it shows about the foreign policy of the United States."

Ads by Google

## Mitt Romney For President

Help Mitt Win The 2012 Election. Join Our Support Campaign Today  
[MittRomneyIn2012.com](#)

## FlodMaster LeakDetection



Protect your valuables from water damage with our auto shutoff system  
[www.floodmaster.com](http://www.floodmaster.com)

#### MS Store Grand Opening

Play Kinect with John Wall Aug. 9 at the Arlington MS Store Opening!  
[www.MicrosoftStore.com/Arlington](http://www.MicrosoftStore.com/Arlington)

#### **We recommend**

Repeal health care law? Forget about it CNN Opinion

What Kim's 'mystery woman' says about North Korea CNN International

Is Sebastian Thrun's Udacity the future of higher education? CNN Opinion

Rep. Jesse Jackson being treated at Mayo Clinic for depression CNN.com

Ugandan officials, international experts tackle Ebola outbreak that's left 14 dead CNN International

Aurora heroes: Three who gave their lives CNN.com

#### **From around the web**

10 Richest Universities in the US TheStreet

Why Aug 1 Could Crush Your Retirement Money Morning

911 Calls Gone Tragically Wrong Reader's Digest

Tour Kinsale Alley's Mains Home for Sale HGTV FrontDoor

We Can't Help But Stare... Sofia Vergara Pictures StyleBistro

"Last Meals" End in Texas Prisons The Daily Meal

[what's this]

# **ATTACHMENT H**



Jump to video

Biden to GOP: 'Let's do the nation's

# Biden on START, WikiLeaks

[Listen](#) [Watch](#) [Discuss](#) [Related](#)

The vice president offered his insight on top political issues

By  
Andrea Mitchell

Host, Andrea Mitchell Reports

MSNBC

## TRANSCRIPT

Vice President Joe Biden sat down with NBC News Chief Foreign Affairs Correspondent Andrea Mitchell to discuss the current state of the war in Afghanistan, debates over the START Treaty, the tax compromise and WikiLeaks. Vice President Biden also offered his heartfelt thoughts on the loss of Richard Holbrooke.

*Read the excerpts below:*

### Biden on the START Treaty and Tax Compromise

**VICE PRESIDENT JOE BIDEN:** Well, I say let's do the nation's business. Sixty-seven senators voted to move forward on this, including John McCain and Lindsey Graham and the leading voices in the Republican Party.

**NBC's ANDREA MITCHELL:** But they say they haven't had enough time to study it.

**BIDEN:** Well, they haven't said that —

**MITCHELL:** No, I —

**BIDEN:** They haven't said that.

**MITCHELL:** — you know, Senator Kyl and the opponents —

**BIDEN:** Senator Kyl is opposed to the treaty. He is flat opposed to the treaty. So is Senator DeMint opposed to the treaty. Do not let — do not stand in the way of the nation's best interests. Let the Senate vote. Overwhelmingly, the American people support the START Treaty. Overwhelmingly, the United States Senate supports the START Treaty. It's clearly in our national interests. Every former national security adviser, secretary of Defense, the secretary of State on the Republican Party from George Shultz to Colin Powell thinks it's essential we pass this treaty. Get out of the way. There's too much at stake for America's national security. And don't tell me about Christmas. I understand Christmas. I have been a senator for a long time. I've been there many years where we go right up to Christmas.

There's 10 days between now and Christmas. I hope I don't get in the way of your Christmas shopping, but this is the nation's business. This is the national security that's at stake. Act. Act.

**MITCHELL:** Does that go for the tax cut, as well?

**BIDEN:** — that we just acted on.

**MITCHELL:** But you had a rough session with House Democrats.

**BIDEN:** Sure, I did.

**MITCHELL:** They say you sold them out, you sat down with Mitch McConnell and you went in the back room and you cut a deal with the Republicans.

**BIDEN:** Hey, look, it's true I did — It's true I did negotiate this package. I was in an interview with another network, I will not mention, not long ago. And they said the Senate said you sold them out and it will never pass. I said more than 80 will vote for it. Eighty senators just voted for that deal I allegedly sold them out on.

**MITCHELL:** Eighty-one.

**BIDEN:** Eighty.

**MITCHELL:** Eighty-one.

**BIDEN:** Well, more than 80. Yes, 80 — 81. The House will, as well. Look, people feel very strongly and I don't blame them. But we cannot afford to go into next year with everyone's taxes going up, the economy threatening to go into a double dip, not growing the economy.

So I had two dictates from the president. Joe, one, make sure whatever you negotiate grows the economy next year. Every major econometric model points out the deal that I was asked to negotiate will increase the growth of the economy from 2.3 to 2.5 to 3.7 to 4. That means tens of thousands, millions of additional jobs.

Secondly, he said to me, Joe, make sure our folks aren't hurt, meaning middle class and working class people. Guess what?

Every one of the tax breaks they had, from college tuition to child care tax credit, which the Republicans opposed, is part of that deal. Every single tax break for middle class Americans has been preserved.

**BIDEN:** Thirdly, it's for two years. We also have a payroll tax where every person next year will get 2 percent less taken out of their payroll. That's real money. That means well over \$1,000 for the average person out there, additional.

**MITCHELL:** But the House Democrats, the liberals, they are the people that brought you into power.

**BIDEN:** Sure they are.

**MITCHELL:** What are you now saying to them?

**BIDEN:** Well, I'll tell you, I went in and spoke to them two-and-a-half hours. I'm a creature of the Congress. When I walked in, I got a standing ovation. When I walked out, I got an ovation. All this talk about how there is this overwhelming contention. Not a single one did not thank me. Not a single one said to me that they thought that I sold anybody out. Not a single one said to me that they thought you were going to be able to decouple the upper income tax from the middle class tax cut.

What their argument was is you should have taken more time, Joe. You should have taken more time. The minority who spoke said that. There were a number of people who stood up and said, this is important. Thank you for the deal you negotiated, including progressives and moderates.

**MITCHELL:** Well, if you were still in the Senate, what about this appropriations bill? All these earmarks and ... Senator McCain was on the floor. He said, you know, you are asleep, to his colleagues, didn't you get the message of the election, people don't want all this pork.

**BIDEN:** Look, we are in a position where, as the president, we don't get to negotiate this. We set out two parameters. We said we wanted to freeze discretionary spending. It is frozen in this omnibus bill.

Two, we said we need additional funding for national security, additional funding for follow-on in Iraq, so to make sure the civilian side gets ramped up and for dealing with international terrorist organizations. We got both of those things. Do we like some of these, quote, earmarks in there?

No, we don't like them. But the question is, as we go to throw out, you know, the baby with the bath water here?

If, in fact, this omnibus bill negotiated by Republicans and Democrats — not by us — Republicans and Democrats — passes, the president will support it.

**Biden on his relationship with Obama and with members of Congress**

**MITCHELL:** And you are the point man on all of this. You're here at the United Nations. You're negotiating with Mitch McConnell. You're everywhere. Are you basically the de facto chief of staff?

**BIDEN:** Well, look, when the president asked me to join him, he asked what portfolio I wanted. I said I want to be in the room when every decision is being made. You're president, but I want to have an input.

And so the president uses me where I have some skill set. I'm going to say something outrageous. They kid me all the time. I still consider myself a Senate man. I love the Senate. I love the Congress. I keep in touch with them.

So I had great relationships with Republicans as well as Democrats. There's real trust. So it's logical for me, at this point, to be a point man in dealing with the House and the Senate at this time.

I have a significant background — I mean I'm good or bad, but I have a significant background in foreign policy and national security issues. So it's logical that I'd come up here. The president asked me, as you know, because you were one of the first people to interview me when he turned to me and said, Joe, you do Iraq. And the Secretary of Defense and the Secretary of State have cooperated with me. They've followed it with me.

I mean, so it was just logical things that I happened to have some experience, in some cases significant experience. And they just happened to be in the two areas that are being negotiated right now.

#### On WikiLeaks

**BIDEN:** I came in, almost all of it was embraces. I mean it wasn't just shaking hands. I know — I know these guys. I know these women. They still trust the United States. There's all kinds of things and —

**MITCHELL:** So there's no damage?

**BIDEN:** I don't think there's any damage. I don't think there's any substantive damage, no. Look, some of the cables that are coming out here and around the world are embarrassing. I mean, you know, to say that, you know, for you to do a cable as an ambassador and say I don't like Biden's tie, he doesn't look good and he's a homely guy, that's not something —

**MITCHELL:** I never said that.

**BIDEN:** No, I know you didn't. I know you didn't. But yet, I mean, you know, there's — so there's a lot of things like that. But nothing that I am aware of that goes to the essence of the relationship that would allow another nation to say they lied to me, we don't trust them, they really are not dealing fairly with us.

#### On Iraq

**MITCHELL:** Iraq — we still have 48,000 troops. Your own son was there. Now another Christmas is coming and they're — they have a government, but there is so much that has not been accomplished.

**BIDEN:** Well, there's been — think of today. You know this place better than most. Today, the international community said, Iraq, you're back in the family of nations. We think you have a government. We think you are moving in the right direction. We think you're protecting human rights. And we think you're going to be stable.

And so we passed through resolutions here in the Security Council — I had the pleasure of presiding over today — which essentially wiped out the restrictions and the claims against Iraq that were imposed after Saddam Hussein went into Kuwait.

And so this is a reaffirmation that Iraq is back. The international community doesn't think there's so long to go. They know there's more work to be done. But they think they have turned the corner, they have a democracy and they're moving forward.

#### Biden on Holbrooke

**MITCHELL:** And, finally, a terrible, terrible loss for all of us, for the country.

**BIDEN:** Richard Holbrooke.

**MITCHELL:** Your thoughts on —

**BIDEN:** I have been —

**MITCHELL:** — having this Afghanistan —

**BIDEN:** — friends —

**MITCHELL:** — review without him.

**BIDEN:** — with Richard, I was a 29-year-old senator-elect. He was a young, 31-year-old Foreign Service officer in Vietnam. I ran opposed to the war against Vietnam — the — excuse me, the war in Vietnam. We became friends and acquaintances way back then.

He was one of the few figures in American foreign policy who was literally larger than life. And I thought — I wish Kati could have heard when we — when I conducted the Security Council meeting. Almost every single member spoke of him before they made their statements about Iraq. And a number of them spoke from personal terms and it was his heart — from their hearts.

No one, as my grandfather would say, it's a good thing about American democracy, is everyone is expendable, in terms of the — the functioning of this great country. But I'll tell you what, it's going to be a long, long time before anybody is big enough to fill Richard's shoes in every way. He was an outsized personality, an outsized talent. And he contributed more to the peace and security of this country as much as anyone in the last 30 years.

**MITCHELL:** And we all know there were moments with him. He could be difficult.

**BIDEN:** He sure could. As a matter of I was with Kati and — at the hospital the day before he died, because I went through a similar kind of event with the aneurisms I had. His was more serious, but they — it was — there was a touch and go place for me for about three months. And so she was asking me, what was it like and will he remember this. And we were talking.

And we started joking. And I said, you know, he can be a real pain in the you know what. And she laughed like hell. And I was kidding her. I said, thank god you were there for the last 17 years to moderate him and then she told me how he would say the same of me.

But we were friends. This was a guy who was — he had a prodigious intellect. He had a sort of a Kissingerian mind. He saw things globally, strategically, like few other men and women I've dealt with. And he could be very, very tough. But he was my friend.

**MITCHELL:** Do you have a Christmas message, a holiday message?

**BIDEN:** Yes. As my grand pop would say, keep the faith. Keep the faith. This country is so strong. It is so big. It is so resilient. Nothing at all can damage its ability to move forward.

A lot of people are hurting. I remember a Christmastime when my dad lost his job and he told us we had to move. It is horrible. But you know what, you know what, we'll come back. And in the meantime, keep in your prayers all those people who are going through really difficult times now.

**MITCHELL:** And our men and women in —

**BIDEN:** And, look —

**MITCHELL:** — combat.

**BIDEN:** — Jill and to be honest with you, I tried to — I had hoped to spend Christmas in Iraq this year, but it was inappropriate to go while the government was still being formed. And so our thoughts and prayers are with us. We had, for Thanksgiving, we had a number of the young men and women who are amputees over for the holidays. We'll spend Christmas at Walter Reed again.

These are incredible, incredible kids. And to all you — all you moms and dads and sons and daughters who have someone in harm's way now, keep them in your prayers. They'll be home next year.

**MITCHELL:** Thank you so very much.

**BIDEN:** Thank you.

© 2012 msnbc.com

New! Share what you're reading & see what your friends are viewing

Allow What's this?

msnbc on Facebook Like

22,470 people like msnbc



Kumar Dymel Smith Walker Rivas Jim Joe Orl Monroe

Pin back social plugin



# **ATTACHMENT I**

*The New York Times***The Lede***Mapping the News With Robert Mackey*

---

JANUARY 19, 2011, 7:45 PM

**U.S. Officials Reportedly Said WikiLeaks Revelations Were 'Not Damaging'**

By ROBERT MACKEY

According to a Congressional aide who spoke to Reuters, State Department officials concluded late last year that the publication of leaked United States diplomatic cables obtained by WikiLeaks "was embarrassing but not damaging."

As the news agency reports, that private assessment, "that a mass leak of diplomatic cables caused only limited damage to U.S. interests abroad," contrasts sharply with the Obama administration's public statements on the potential harm of the WikiLeaks disclosures.

P.J. Crowley, a State Department spokesman, reiterated that public stance, telling the news agency, "From our standpoint, there has been substantial damage." He added: "We believe that hundreds of people have been put at potential risk because their names have been compromised in the release of these cables."

The reported reversal by the State Department is strikingly similar to a Pentagon volte-face on a prior WikiLeaks release.

As my colleague Elisabeth Bumiller reported in October, "Defense Secretary Robert M. Gates said in a private letter over the summer that while the release of 75,000 classified documents about the war in Afghanistan by the Web site WikiLeaks endangered the lives of Afghans helping the United States, the disclosures did not reveal any significant national intelligence secrets."

In his letter, dated Aug. 16, Mr. Gates assured the chairman of the Senate Armed Services Committee, Senator Carl Levin, "the review to date has not revealed any sensitive intelligence sources and methods compromised by this disclosure." At a Pentagon news conference barely two weeks earlier, Mr. Gates had insisted that the leaks were damaging because "intelligence sources and methods" detailed in the Afghan war documents published by WikiLeaks "will become known to our adversaries."

At the same briefing, the chairman of the Joint Chiefs of Staff, Adm. Mike Mullen, went even further, saying, "Mr. Assange can say whatever he likes about the greater good he thinks he and his source are doing, but the truth is they might already have on their hands the blood of some young soldier."

Oddly, the private comments reportedly made by State Department officials on the leaked cables match almost exactly a public statement on them made by none other than Mr. Gates in November:

Mr. Gates, who is also a former C.I.A. director, told reporters then:

Let me just offer some perspective as somebody who's been at this a long time. Every other government in the world knows the United States government leaks like a sieve, and it has for a long time. And I dragged this up the other day when I was looking at some of these prospective releases. And this is a quote from John Adams: 'How can a government go on, publishing all of their negotiations with foreign nations, I know not. To me, it appears as dangerous and pernicious as it is novel.'

When we went to real Congressional oversight of intelligence in the mid-70s, there was a broad view that no other foreign intelligence service would ever share information with us again, if we were going to share it all with the Congress. Those fears all proved unfounded.

Now, I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer, and so on. I think those descriptions are fairly significantly overwrought.

The fact is, governments deal with the United States because it's in their interest, not because they like us, not because they trust us, and not because they believe we can keep secrets. Many governments - some governments - deal with us because they fear us, some because they respect us, most because they need us. We are still essentially, as has been said before, the indispensable nation.

So other nations will continue to deal with us. They will continue to work with us. We will continue to share sensitive information with one another.

Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest.

**ESPIONAGE ACT AND THE LEGAL AND  
CONSTITUTIONAL ISSUES RAISED BY WIKILEAKS**

---

**HEARING**  
BEFORE THE  
**COMMITTEE ON THE JUDICIARY**  
**HOUSE OF REPRESENTATIVES**  
**ONE HUNDRED ELEVENTH CONGRESS**  
**SECOND SESSION**

DECEMBER 16, 2010

**Serial No. 111-160**

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

U.S. GOVERNMENT PRINTING OFFICE  
WASHINGTON : 2011

63-081 PDF

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800, DC area (202) 512-1800  
Fax: (202) 512-2104 Mail Stop IDCC, Washington, DC 20402-0001

# COMMITTEE ON THE JUDICIARY

JOHN CONYERS, Jr., Michigan, *Chairman*

HOWARD L. BERMAN, California	LAMAR SMITH, Texas
RICK BOUCHER, Virginia	F. JAMES SENSENBRENNER, Jr., Wisconsin
JERROLD NADLER, New York	HOWARD COBLE, North Carolina
ROBERT C. "BOBBY" SCOTT, Virginia	ELTON GALLEGLY, California
MELVIN L. WATT, North Carolina	BOB GOODLATTE, Virginia
ZOE LOFGREEN, California	DANIEL E. LUNGREN, California
SHEILA JACKSON LEE, Texas	DARRELL E. ISSA, California
MAXINE WATERS, California	J. RANDY FORBES, Virginia
WILLIAM D. DELAHUNT, Massachusetts	STEVE KING, Iowa
STEVE COHEN, Tennessee	TRENT FRANKS, Arizona
HENRY C. "HANK" JOHNSON, Jr., Georgia	LOUIE GOHMERT, Texas
PEDRO PIERLUISI, Puerto Rico	JIM JORDAN, Ohio
MIKE QUIGLEY, Illinois	TED POE, Texas
JUDY CRU, California	JASON CHAFFETZ, Utah
TED DEUTCH, Florida	TOM ROONEY, Florida
LUIS V. GUTIERREZ, Illinois	GREGG HARTER, Mississippi
TAMMY BALDWIN, Wisconsin	
CHARLES A. GONZALEZ, Texas	
ANTHONY D. WEINER, New York	
ADAM B. SCHIFF, California	
LINDA T. SANCHEZ, California	
DANIEL MAPPEI, New York	
JARED POLIS, Colorado	

PERRY APPELBAUM, *Majority Staff Director and Chief Counsel*  
 SEAN McLAUGHLIN, *Minority Chief of Staff and General Counsel*

# CONTENTS

DECEMBER 16, 2010

Page

## OPENING STATEMENTS

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary	1
The Honorable Louie Gohmert, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	3
The Honorable William D. Delahunt, a Representative in Congress from the State of Massachusetts, and Member, Committee on the Judiciary	4
The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Member, Committee on the Judiciary	5
The Honorable Charles A. Gonzalez, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	5
The Honorable Ted Poe, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary	5

## WITNESSES

Mr. Geoffrey R. Stone, Professor and former Dean, University of Chicago Law School	6
Oral Testimony	9
Prepared Statement	9
Mr. Abbe David Lowell, Partner, McDermott Will & Emery, LLP	22
Oral Testimony	22
Prepared Statement	25
Mr. Kenneth L. Wainstein, Partner, O'Melveny & Myers, LLP	39
Oral Testimony	39
Prepared Statement	41
Mr. Gabriel Schoenfeld, Ph.D., Senior Fellow, Hudson Institute	48
Oral Testimony	48
Prepared Statement	50
Mr. Stephen I. Viadeck, Professor of Law, American University	66
Oral Testimony	66
Prepared Statement	68
Mr. Thomas S. Blanton, Director, National Security Archive, George Washington University	74
Oral Testimony	74
Prepared Statement	77
Mr. Ralph Nader, Legal Advocate and Author	87
Oral Testimony	87

## ESPIONAGE ACT AND THE LEGAL AND CONSTITUTIONAL ISSUES RAISED BY WIKILEAKS

THURSDAY, DECEMBER 16, 2010

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Committee met, pursuant to notice, at 10:05 a.m., in room 2141, Rayburn House Office Building, the Honorable John Conyers, Jr. (Chairman of the Committee) presiding.

Present: Representatives Conyers, Scott, Jackson Lee, Delahunt, Johnson, Quigley, Gutierrez, Schiff, Sensenbrenner, Coble, Gallegly, Goodlatte, King, Frank, Gohmert, Poe, and Harper.

Staff Present: (Majority) Perry Apfelbaum, Staff Director and Chief Counsel; Elliot Minberg, Counsel; Sam Sokol, Counsel; Joe Graupensberger, Counsel; Nafees Syed, Staff Assistant; (Minority) Caroline Lynch, Counsel; Kimani Little, Counsel; and Kelsey Whitlock, Clerk.

Mr. CONYERS. Good morning. The hearing on the Espionage case and the legal and constitutional issues raised by WikiLeaks before the Committee on Judiciary is now about to take place. We welcome everyone here to the hearing. In the *Texas v. Johnson* case in 1989, the Supreme Court set forth one of the fundamental principles of our democracy. That is, that if there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable.

That was Justice William Brennan. Today the Committee will consider the WikiLeaks matter. The case is complicated, obviously. It involves possible questions of national security, and no doubt important subjects of international relations, and war and peace. But fundamentally, the Brennan observation should be instructive.

As an initial matter, there is no doubt that WikiLeaks is in an unpopular position right now. Many feel their publication was offensive. But unpopularity is not a crime, and publishing offensive information isn't either. And the repeated calls from Members of Congress, the government, journalists, and other experts crying out for criminal prosecutions or other extreme measures cause me some consternation.

Indeed, when everyone in this town is joined together calling for someone's head, it is a pretty sure sign that we might want to slow down and take a closer look. And that is why it was so encouraging

to hear the former Office of Legal Counsel, Jack Goldsmith, who served under George W. Bush caution us only last week. And he said, I find myself agreeing with those who think Assange is being unduly vilified. I certainly do not support or like his disclosure of secrets that harm U.S. national security or foreign policy interests. But as all the handwringing over the 1917 Espionage Act shows, it is not obvious what law he has violated.

Our country was founded on the belief that speech is sacrosanct, and that the answer to bad speech is not censorship or prosecution, but more speech. And so whatever one thinks about this controversy, it is clear that prosecuting WikiLeaks would raise the most fundamental questions about freedom of speech about who is a journalist and about what the public can know about the actions of their own government.

Indeed, while there's agreement that sometimes secrecy is necessary, the real problem today is not too little secrecy, but too much secrecy. Recall the Pentagon papers case, Justice Potter Stewart put it, when everything is classified, nothing is classified. Rampant overclassification in the U.S. system means that thousands of soldiers, analysts and intelligence officers need access to huge volumes of purportedly classified material. And that necessary access in turn makes it impossible to effectively protect truly vital secrets.

One of our panelists here today put it perfectly in a recent appearance. He explained, our problem with our security system, and why Bradley Manning can get his hands on all these cables, is we got low fences around a vast prairie because the government classifies just about everything. What we really need are high fences around a small graveyard of what is really sensitive. Furthermore, we are too quick to accept government claims that risk the national security and far too quick to forget the enormous value of some national security leaks. As to the harm caused by these releases most will agree with the Defense Secretary, Bob Gates, his assessment.

Now, I have heard the impact of these releases on our foreign policy described as a meltdown, as a game changer, and so on. I think those descriptions are fairly significantly overwrought. And Mr. Gates continues, is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. policy? I think fairly modest.

So the harm here, according to our Republican Defense Secretary, is fairly modest. Among the other side of the ledger, there is no need to go all the way back to the Pentagon papers to find examples of national security leaks that were critical to stopping government abuses and preserving a healthy democracy. They happen all the time.

In 2005, The New York Times published critical information about widespread domestic surveillance. Ultimately, we learned of a governmental crisis that included threats of mass resignations at the Justice Department and outrageous efforts to coerce a sick attorney general into approving illegal spying over the objections of his deputy and legal counsel's office. If not for this leak, we would have never learned what a civil libertarian John Ashcroft is.

In 2004, the leak of a secret office of legal counsel interrogation memos led to broader revelations of the CIA's brutal enhanced interrogation programs at Black sites. These memos had not been



previously revealed to the Judiciary Committee or to many in Congress. Some feel this harmed national security. But to many Americans, the harm was a secret program of waterboarding and other abuses that might never have been ended but for the leak.

And so we want to, as the one Committee in the Congress that I have a great and high regard for, take a closer look at the issues and consider what, if any, changes in the law might be necessary. And I want to welcome this very distinguished panel. I have read late into the night, and I was awake most of the time when I was reading this, some really great testimony. And I am so glad that you are all here with us. I would like now to recognize my friend and Ranking Member, Judge Louie Gohmert.

Mr. GOHMERT. Thank you, Chairman. And I do appreciate the witnesses here. Before I begin my actual statement, let me just say I appreciate, and am also intrigued by your metaphorical use of the need for high fences around a small graveyard. But I am curious, are you saying this Administration is located in a small graveyard? Is that the point?

Mr. CONYERS. See me after the hearing, please, Judge Gohmert.

Mr. GOHMERT. Thank you, Chairman. And I appreciate the Ranking Member Smith asking me to stand in. But the release last month by WikiLeaks of over 250,000 classified and diplomatic U.S. documents threatens our national security, our relations with foreign governments, and continued candor from embassy officials and foreign sources. Many have applauded the Web site and its founder, Julian Assange, as a hero advocating the continued release of classified and sensitive government documents. But to do so is both naive and dangerous. Web sites such as WikiLeaks and the news publications that reprint these materials claim to promote increased government transparency.

But the real motivation is self-promotion and increased circulation to a large extent. They claim to be in pursuit of uncovering government wrongdoing but dismiss any criticism that their actions may be wrong or damaging to the country. As long as there have been governments, there have been information protected by those governments. There have clearly been documents classified that should not have been classified. While there is legitimate dispute over the extent to which information is protected and classified, it is simply unrealistic to think that the protection of information serves no legitimate purpose.

Much attention has been given to this most recent WikiLeaks release. Many dismiss that any negative repercussions resulted from the leak arguing that the documents, while embarrassing to the U.S., did no real harm to the country. But what about previous leaks by this Web site? On July 25, 2010, WikiLeaks released confidential military field reports on the war in Afghanistan. This site released Iraq war-related documents on October 23, 2010. Both of these leaks reveal sensitive military information that endangers military troops and may have bolstered our enemy's campaigns against us.

Last month's WikiLeaks release has thrust in the spotlight an old, some would even say, arcane statute, the Espionage Act of 1917. It has also resurrected an age-old debate on First Amendment protections afforded to media publications.

$\gamma_0$ 

**GOVERNMENT RESPONSE TO  
DEFENSE MOTION FOR  
JUDICIAL NOTICE AND ADMISSION  
OF PUBLIC STATEMENTS**

17 August 2012

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny, in part, the Defense Motion for Judicial Notice and Admission of Public Statements. The United States does not object to this Court taking judicial notice that statements were made by some of the individuals listed in the defense motion.

As the moving party, the defense has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM), United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2012). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

1. The United States stipulates to the facts set forth in paragraphs 3 and 4 of the Defense Motion.
2. The United States does not object to this Court taking judicial notice that statements were made by the individuals listed below. *See* Def. Mot. at 2-4.
  - a. Paragraph 2a of the Defense Motion (Statement of Geoff Morrell, Pentagon Press Secretary)
  - b. Paragraph 2b of the Defense Motion (Statement of President Barack Obama), provided the Court takes judicial notice of the entire statement quoted in the article provided by the defense at Attachment B.
  - c. Paragraph 2c of the Defense Motion (Statement of Secretary of Defense Robert Gates)
  - d. Paragraph 2c of the Defense Motion (Statement of Secretary of State Hillary Rodham Clinton)
  - e. Paragraph 2c of the Defense Motion (Statement of Vice President Joseph R. Biden)

3. The United States objects to this Court taking judicial notice that any other "statements" were made by the individuals listed in the defense motion.

### WITNESSES/EVIDENCE

The United States requests this Court consider the referred Charge Sheet in support of its response.

### LEGAL AUTHORITY AND ARGUMENT

The defense requests this Court take judicial notice that the remaining listed statements were made by the attributed individuals because they are capable of accurate and ready determination via "a quick web search." See Def. Mot. at 4. However, the defense has provided no reliable evidence to this Court that the remaining "statements" were made by the attributed individuals as they are quoted in the defense motion.

A judicially noticed fact "must be one not subject to reasonable dispute in that it is either (1) generally known universally, locally, or in the area pertinent to the event or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Military Rule of Evidence (MRE) 201(b). Judicial notice of facts serves as a substitute for testimonial, documentary, or real evidence. Stephen A. Saltzburg, et al., *Military Rules of Evidence Manual* § 201.02[1] (7th ed. 2011). Additionally, judicial notice promotes judicial economy because it relieves a proponent from formally proving certain facts that a reasonable person would not dispute. *Id.*

Because judicial notice of facts is a substitute for proving the fact, courts use judicial notice cautiously to avoid depriving a party of the opportunity to use rebuttal evidence, cross-examination, and argument to attack contrary evidence. See *American Prairie Construction Company v. Hoich*, 560 F.3d 780, 797 (8th Cir. 2009). Judicial notice cannot be used in contravention of the relevancy, foundation, and hearsay rules. See *id.* at 797 (noting that each judicially noticed document included hearsay evidence which is generally only admissible at trial through an enumerated hearsay exception) (citing *Baker v. Barnhart* 457 F.3d 882, 890-92 (8th Cir. 2006)). Where the matter is in controversy, judicial notice is inappropriate and the traditional rules of evidence should be applied. See *Holloway v. Lockhart*, 813 F.3d 874, 878-79 (8th Cir. 1987) (deciding that determining whether use of tear gas against inmates was a reasonable decision could not be judicially noticed and should be evaluated by the testimony and credibility of various witnesses).

The courts have not defined a rule delineating when the full rules of evidence must be used in place of judicial notice. Essentially, "[f]acts of universal notoriety need not be proved." *Brown v. Piper*, 91 U.S. 37, 42 (1875). For instance, facts deemed unreliable because of age and hearsay cannot be judicially noticed. See *United States v. Hale*, 978 F.2d 1016, 1021 (8th Cir. 1992) (declining to take judicial notice of Senate subcommittee hearing transcripts because the ten year old transcripts were hearsay and too old to be deemed reliable). Reliance on primary sources such as treatises and scientific journals that are deemed trustworthy creates an adequate

basis for taking judicial notice of an adjudicative fact. *See Brown*, 33 M.J. at 710 (holding that an article concerning trial tactics and judicial theory was not proper for judicial notice). Ultimately, the moving party must meet the statutory test and demonstrate that the facts to be noticed judicially are generally known or universally accepted as accurate. *United States v. Coleman*, 32 M.J. 508, 511 (A.C.M.R. 1990).

## **GOVERNMENT OBJECTIONS TO JUDICIAL NOTICE OF CERTAIN STATEMENTS**

The United States objects to this Court taking judicial notice of either of the “statements” made by Marine Corps Colonel David Lapan. First, what the defense has listed in its motion could hardly be characterized as a “statement.” Second, neither Attachment C nor Attachment D to the Defense Motion provide any evidence that Col. Lapan made any statement remotely approaching what the defense has proffered in its motion.

The United States also objects to this Court taking judicial notice of any statement made by Defense Secretary Robert Gates in a 16 August 2010 letter to the Chairman of the Senate Armed Services Committee. *See* Def. Mot. at 2. A court may take judicial notice of an adjudicative fact if it is capable of “accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” MRE 201(b)(2). In this case, the defense has not provided this Court the letter sent by Secretary Gates, but instead has provided an internet news article reporting on the letter allegedly sent. The article provided by the defense does not quote the letter in full.

Additionally, the United States objects to this Court taking judicial notice of the “statement” made by Secretary Clinton in Attachment G to the Defense Motion. *See* Def. Mot. at 3. The defense provides this Court an internet news article from CNN.com, which acknowledges that Secretary Clinton made comments off-camera but on the record. The article quotes various comments made by Secretary Clinton while aboard her plane, but it is difficult to determine where certain statements begin and end as the article undoubtedly quoted Secretary Clinton as she spoke extemporaneously with reporters. The CNN.com article can hardly be characterized as a “source whose accuracy cannot reasonably be questioned.” MRE 201(b).

Finally, the United States objects to this Court taking judicial notice of the statement made by Representative John Conyers, Jr., at a congressional hearing on 16 July 2010. *See* Def. Mot. at 3. The defense has provided no evidence that Representative Conyers made that statement. Instead, Attachment I to the Defense Motion is an article from an internet blog of *The New York Times* that does not even mention Representative Conyers.

## **THE STATEMENTS ARE NOT ADMISSIBLE UNDER MRE 801(D)(2)**

Hearsay “is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.” MRE 801(c). Unless authorized as an exception, hearsay is inadmissible. MRE 802. Admissions by party-opponents are recognized as statements that are not hearsay. *See* MRE 801(d)(2). Admissions by a party-opponent include a statement that is offered against a party and is “(A) the party’s own statement in either the party’s individual or a representative capacity, or (B) a statement of which the party

has manifested the party's adoption or belief in its truth, or ... (D) a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship . . . ." MRE 801(d)(2).

The defense contends that all the statements are admissible under MRE 801(d)(2)(B) and 801(d)(2)(D) because they were made by an individual who "either serves as a high-level government bureaucrat, heading a government agency with the ability to bind the government through policy-making decisions, or, as part of his employment, spoken [sic] on behalf of those who did/do have the ability to bind the sovereign," and cites a D.C. District Court telephone antitrust action as the main support for its proposition. Def. Mot. at 6; see *United States v. American Tel. & Tel. Co.*, 498 F. Supp. 353 (D.C.D.C. 1980). The defense also looks to *United States v. Kattar*, which potentially limits the holding in *American Telephone & Telegraph Company*. *United States v. Kattar*, 840 F.2d 118, 130-31 (1st Cir. 1988) ("Whether or not the entire federal government in all its capacities should be deemed a party-opponent in criminal cases, cf. *United States v. American Tel. & Tel.*, 498 F. Supp. 353, 356-58 (D.D.C.1980) (civil case), the Justice Department certainly should be considered such."). Furthermore, the First Circuit does not hold that statements by alleged government agents are admissible as statements of party opponents under Rule 801(d)(2). See *Kattar*, 840 F.2d at 118. The court found that the Justice Department was the party opponent under Rule 801(d)(2)(B) and its statements made in a formal prosecution "establish the position of the United States and not merely the views of its agent who participate therein." *Id.* at 131 (citing *United States v. Powers*, 467 F.2d 1089, 1097 n.1 (7th Cir. 1972) (Stevens, J., dissenting)). In its limited finding, the court noted that "[t]he government cannot indicate to one federal court that certain statements are trustworthy and accurate, and then argue to a jury in another federal court that those same assertions are hearsay." *Kattar*, 840 F.2d at 131.

Not only is the defense's position untenable, but it is not supported by case law. Other federal circuit courts have repeatedly held that government agents are not party-opponents. See *United States v. Arroyo*, 406 F.3d 881, 888 (7th Cir. 2005) ("This Court has held that government agents are not party-opponents for purposes of Rule 801(d)(2)"); see also *United States v. Booker*, 375 Fed. Appx. 225, 230-31 (3d Cir. 2010) ("Here, the party-opponent is the United States. . . . several courts, including, ours, 'have held that statements by police officers or other law enforcement officials are not admissible on an admissions theory as substantive evidence against the sovereign in a criminal prosecution.'") (quoting *Lippay v. Christos*, 996 F.2d 1490, 1497 (3d Cir. 1993)); *United States v. Kapp*, 781 F.2d 1008, 1014 (3d Cir. 1986) ("There is no authority for the proposition that the prosecution is a 'party' against whom such [Rule 801(d)(2)] evidence can be offered.").

*United States v. Kampiles* is also instructive on this point. *United States v. Kampiles*, 609 F.2d 1233, 1246 (7th Cir. 1979), cert. denied, 446 U.S. 954, 100 S. Ct. 2923 (1980). In *Kampiles*, the defense tried to offer the statement of a former CIA employee as the statement of a party opponent under Rule 801(d)(2)(D). *Id.* In ruling against the defense, the Seventh Circuit explained why Federal Rule of Evidence 801(d)(2) is not imputed onto government agents. Prior to the adoption of the Federal Rules of Evidence, "admissions by government employees in criminal cases were viewed as outside the admissions exception to the hearsay rule." *Id.* at 1246 (citing *United States v. Powers*, 467 F.2d 1089, 1095 (7th Cir. 1972); see also *United States v.*


*Santos*, 372 F.2d 177, 180 (2d Cir. 1967) ("Though a government prosecution is an exemplification of the adversary process, nevertheless, when the Government prosecutes, it prosecutes on behalf of all the people of the United States; therefore all persons, whether law enforcement agents, government investigators, complaining prosecuting witnesses, or the like, who testify on behalf of the prosecution, and who, because of an employment relation or other personal interest in the outcome of the prosecution, may happen to be inseparably connected with the government side of the adversary process, stand in relation to the United States and in relation to the defendant no differently from persons unconnected with the effective development of or furtherance of the success of, the prosecution. Therefore, the inconsistent out-of-court statements of a government agent made in the course of the exercise of his authority and within the scope of that authority, which statements would be admissions binding upon an agent's principal in civil cases, are not so admissible here as 'evidence of the fact.'").

According to the *Kampiles* court, "[b]ecause the agents of the Government are supposedly disinterested in the outcome of a trial and are traditionally unable to bind the sovereign, . . . their statements seem less the product of the adversary process and hence less appropriately described as admissions of a party." *Kampiles*, 609 F.2d at 1246 (citing *Santos*, 372 F.2d at 180). The court determined that "[n]othing in the Federal Rules of Evidence suggests an intention to alter the traditional rule." *Kampiles*, 609 F.2d at 1246.


As such, all of the statements cited by the defense, which were allegedly made by an individual who "either serves as a high-level government bureaucrat, heading a government agency with the ability to bind the government through policy-making decisions, or, as part of his employment, spoken on behalf of those who did/do have the ability to bind the sovereign" should not be admissible under MRE 801(d)(2).

### CONCLUSION

For the reasons stated above, the United States respectfully requests this Court deny, in part, the Defense Motion for Judicial Notice and Admission of Public Statements.




ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel



JOëAN MORROW  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Defense Counsel,  
via electronic mail, on 17 August 2012.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

FOR OFFICIAL USE ONLY

UNITED STATES OF AMERICA )

v. )

Prosecution Witness List

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

14 August 2012

The United States may call the following witnesses to testify at the Article 13 motion hearing of the above-captioned court-martial:

1. CWO4 James Averhart, Navy Consolidated Brig Chesapeake, Chesapeake, VA, 23322, (707) 421-8672
2. CWO2 Denise Barnes, Deputy Command Inspector General, Marine Corps Base Quantico (MCBQ), Quantico, VA, 22134, (703) 432-0049
3. MSgt Craig Blenis, Security Battalion, Camp Pendleton, CA, 92055, (760) 725-8567
4. CPT Joseph Casamatta, 2d Battalion, 346th Regiment, Camp Shelby, MS, 39407, (703) 399-1730
5. Col (R) Daniel Choike (currently on terminal leave), Technology Associates, McLean, VA, 22101, daniel.choike@taic.net
6. LCpl Jonathan Cline, Headquarters Security Battalion, Quantico, VA, 22134, (781) 956-2406
7. COL Carl Coffman, United States Forces-Afghanistan, carl.coffman@us.army.mil
8. GySgt William Fuller, Headquarters Marine Corps (HQMC), Arlington, VA, 22204, (703) 604-4138
9. CWO5 Abel Galaviz, Security and Law Enforcement Branch, Security Division, Corrections Section, Arlington, VA, 22204, (703) 604-4503
10. SSG Ryan Jordan, United States Army Recruiting Command, ryan.jordan4@us.army.mil
11. MSgt Brian Papakie, HQMC, Arlington, VA, 22204, (703) 604-4129
12. CAPT (R) Jonathan Richardson (currently on terminal leave), Oceanside, CA, 92049, (760) 725-1555
13. LTC Robert Russell, Joint Task Force Guantanamo Bay (JTF-GTMO) (will be departing for JTF-GTMO on or about 22 September 2012), robert.k.russell.mil@health.mil



FOR OFFICIAL USE ONLY

14. Mr. Joshua Tankersly, Gray Court, SC, 29645, (864) 684-9840
15. GM1 Terrance Webb, Navy Munitions Command, CONUS East Division, Detachment Sewells Point, Norfolk, VA, 23513, (757) 443-0800
16. LCDR Eve Weber, Naval Academy Annapolis, Annapolis, MD, 21402, eve.weber@med.navy.mil
17. 1SG Bruce Williams, Headquarters and Headquarters Company, United States Army Garrison, Joint Base Myer-Henderson Hall, VA, 22211, (703) 696-3409

The United States reserves the right to supplement this witness list based on the defense's supplemental witness list, and supplemental motion.

If the defense intends to produce a witness who is listed above, the defense must provide a separate, appropriate request for that witness in accordance with Rule for Courts-Martial (RCM) 703 and the standard articulated in United States v. Rockwood, 52 M.J. 98, 105 (1999) that a witness request include a "synopsis of expected testimony," not merely a list of topics to be covered. If necessary for a particular witness employed by the United States Government, the defense shall also comply with 5 U.S.C. § 301 and Touhy v. Ragen, 340 U.S. 462 (1951).



ALEXANDER VON ELTEN  
CPT, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 14 August 2012.



ALEXANDER VON ELTEN  
CPT, JA  
Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

**MANNING, Bradley E., PFC**

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE REQUESTED  
WITNESSES: ARTICLE 13  
MOTION**

DATED: 15 August 2012

1. On behalf of PFC Bradley E. Manning, his civilian counsel, David E. Coombs requests the attendance of the following additional witnesses for purpose of his Article 13 motion:

- a) LtGen. George J. Flynn, george.j.flynn@usmc.mil, Director for Joint Force Development, The Joint Staff J-7. LtGen. Flynn is the former Commanding General of Marine Corps Combat Development Command. As the Commanding General, he was the senior rater for Col. Daniel Choike, the former Marine Corps Base Quantico (MCBQ) Commander and Col. Robert Oltman, the former MCBQ Security Battalion Commander. LtGen. Flynn will testify about requiring the Quantico Brig to report to him, for his approval, regarding any change in PFC Manning's handling instructions or assignment status. LtGen. Flynn will testify that prior to any final action taken place with changing PFC Manning's custody status, he wanted to be able to determine the political impact, media interest, legal ramifications, and senior leadership reactions. LtGen. Flynn will testify that he received frequent reports, at least once a week, on PFC Manning and his custody status. LtGen. Flynn will testify that he first made inquiries into PFC Manning within a week of his arrival at MCBQ. He will testify that he was concerned about the suicide risk of PFC Manning. He will testify that the Brig had a suicide on 31 January 2010. Based upon the previous suicide he directed Col. Choike and Col. Oltman to impress "upon all who come in contact with Pvt. Manning the absolute necessity of keeping a close watch on him... His [PFC Manning] life has completely fallen apart which makes him a strong candidate (from my perspective) to take his life." Finally, LtGen. Flynn will recount how he became involved in the day to day issues regarding PFC Manning.
- b) Col. Christopher Miner, christopher.miner@usmc.mil, (76) 846-3734, Staff Judge Advocate, 1 Marine Expeditionary Force, Camp Pendleton, CA. Deployed to Afghanistan. Col. Miner is currently on R&R leave. He will testify that he was the SJA for LtGen. Flynn. He will testify that he received regular briefs from LtCol. Greer, Col. Oltman, and Col. Choike regarding PFC Manning. Based upon the briefs he received from others, Col. Miner would provide advice to LtGen. Flynn regarding PFC Manning. Col. Miner was included upon emails where Col. Oltman informed the command that the Brig OIC, CWO4 Averhart, was holding PFC Manning on Suicide Risk (SR) after the mental health professionals had recommended his status be changed from SR to

**APPELLATE EXHIBIT** 210  
**PAGE REFERENCED:**  
**PAGE** \_\_\_ **OF** \_\_\_ **PAGES**

Prevention of Injury (POI). Col. Miner will testify that he was aware of the level of involvement by LtGen. Flynn in the custody status of PFC Manning.

- c) Col. (R) Daniel Choike, Technology Associates, McLean, VA, 22101, daniel.choike@taic.net. Col. (R) Choike will testify regarding his level of involvement in the custody status of PFC Manning. Col. (R) Choike was receiving weekly reports from Col. Oltman and Capt. Neil regarding PFC Manning. Col. (R) Choike subsequently provided weekly reports to LtGen. Flynn. He will testify that he provided immediate reports to LtGen. Flynn that could have any media impact or portray the MCBQ in a negative light. Col. (R) Choike will testify that he was aware of a recommendation by LtCol. Troy Wright, the then Head of Law Enforcement and Corrections Brand for Headquarters, U.S. Marine Corps, to have Army Corrections take a second look at the custody classification of PFC Manning. LtCol. Wright had pointed out that one of the complaints that received a lot of press in how PFC Manning was being held in MAX custody status. LtCol. Wright believed, just like a competent doctor who has confidence in his own work would recommend that a patient get a second opinion, having Army Corrections review the Brig's decisions should not be a problem. Col. (R) Choike will testify that he along with Col. Oltman directed that the visit be cancelled. Col. (R) Choike will also testify that he instructed Col. Oltman that any changes in PFC Manning's custody status must be approved by LtGen. Flynn. Col. (R) Choike will testify that he personally called CWO2 Barnes to let her know about LtGen. Flynn's intent regarding PFC Manning. He told CWO2 Barnes and Col. Oltman that any decision regarding a change in handling instructions or assignment status without first obtaining LtGen. Flynn's approval was not acceptable. Col. (R) Choike told Col. Oltman that LtGen. Flynn wanted to be able to determine the political impact, media interest, legal ramifications, and senior leadership reactions to any decision regarding PFC Manning. Col. (R) Choike will testify that he told Col. Oltman that he would not be able to receive a non-concurrence from LtGen. Flynn in writing as Col. Oltman had requested. Instead, he would simply have to follow the chain of command and adhere to the orders of LtGen. Flynn. Finally, he will testify about his involvement in recommending denial of the multiple Article 138 complaints by PFC Manning.
- d) CDR Han Bui, han.bui@med.navy.mil, Building IA Floor 2, Room 9, Norfolk, VA 23511 (757) 953-0515. CDR Bui will testify that he believed the MCBQ was hypersensitive after the suicide of an inmate in January of 2010. He will testify that he believed that CWO2 Barnes, Col. Oltman, and Col. Choike needed to understand that there was a big difference between what they wanted behavioral health to do at the Brig and what they actually needed. He will testify that he felt it was important to inform and educate his Marine counterparts about what was medically and psychologically appropriate for the care for PFC Manning. He will further testify that it bothered him that the Brig and other key leaders were "playing half-doctor" with the care of PFC Manning. Specifically, he will testify that he did not believe it was appropriate for the brig to place PFC Manning on "suicide watch" without consulting him and then wait for the psychiatrist a few days later to recommend taking him off of suicide watch.

- e) Capt. Mary Neill, mary.neill@med.navy.mil, Capt. Neill is the former commander of the Naval Health Clinic at MCBQ. She will testify that Col. Choike ordered her to provide him with a weekly update on PFC Manning. She will testify that she complied with this order by providing at least weekly reports to Col. Choike. Capt. Neill will testify that the Brig psychiatrists would provide her with a weekly report that she would then add to for the benefit of Col. Choike and Lt.Gen Flynn. Within the report, she would discuss the results of the behavioral health visits, the recommendation of the Brig psychiatrists, the nature of PFC Manning's custody status, and PFC Manning's overall affect and mood. She will testify that she was aware of the Brig psychiatrists, Capt. William Hocter and COL Robert Malone's consistent recommendations to remove PFC Manning from POI watch. Despite their frequent recommendations, PFC Manning was never removed from POI. Capt. Neill will testify that Col. Oltman had come to her to express his loss of trust in the recommendations of Capt. Hocter. She will testify that Col. Oltman blamed Capt. Hocter for failing to identify the individual who committed suicide in January of 2010 as a potential suicide risk. She will testify that she was aware that the Brig had displayed significant concern and was very anxious about the high level of visibility regarding PFC Manning and the associated risks. Capt. Neill believed that the Brig staff would benefit from having some of their questions and concerns addressed by her medical staff. She will also testify that she informed Col. Choike and Col. Oltman that it was her opinion that the continuation of POI was not detrimental to PFC Manning. Capt. Neill will testify that she was also aware of Capt. Hocter's repeated requests for the Brig to allow PFC Manning the opportunity to exercise in his cell. She will testify that Capt. Hocter had noted a decline in the physical conditioning of PFC Manning due to his limited opportunities to be out of his cell. She also will testify that she took it upon herself to have a face to face meeting with the Capt. Brian Moore, the former Defense forensic psychiatrist expert, to inform him that his access to PFC Manning was only through the defense counsel channels, and that he since his appointment to the Defense team, he was no longer part of behavioral health provider team for PFC Manning.
- f) LtCol. Christopher M. Greer, christopher.m.greer@usmc.mil, 1 Cherry Point, Marine Corps Air Station, Cherry Point, NC. LtCol. Greer is currently on PCS leave until 20 August 2012. He will testify that he was present for the meeting where Col. Oltman stated that PFC Manning would remain in his current status Maximum Custody and POI unless and until he received instructions from higher authority to the contrary. LtCol. Greer will testify that he did not attempt to intervene or correct Col. Olman when he told Capt. Hocter something to the effect of "I will not have anything happen to Manning on my watch. So, nothing is going to change in his custody status. He won't be able to hurt himself and he won't be able to get away, and our way of making sure of that is that is he will remain on Maximum Custody and POI indefinitely." LtCol. Greer will testify that Capt. Hocter became upset and expressed his concern about holding PFC Manning in POI when there was no behavioral health justification for such a status. He will testify that Capt. Hocter did not support the POI status, but was told that his recommendation was just a part of the overall classification assessment. He will testify that Col. Oltman told Capt. Hocter that he should just make his recommendations and that they (the confinement facility) would do what they wanted to do. LtCol. Greer will also testify that he provided regular updates to Col. Choike, Col. Oltman, and LtGen. Flynn's SJA

(Col. Christopher Miner) about PFC Manning. Finally, LtCol. Greer will testify that he was aware of a request by the Defense to the Convening Authority, COL Coffman, to remove PFC Manning from POI. He will testify that he informed Col. Choike and Col. Oltman to "stand by for heavy rolls if the CA decides to request the Base commander to review and consider removing Manning's POI status." He will also testify that he informed the Army that "unless you want to run our Brig, I think you undercut your own legal position if you actually recommend that the POI status be removed. We are the jailors, either you trust us or you don't. If you don't, then move him." LtCol. Greer also will testify that he informed the prosecution that "we (the marines) have the day to day responsibility for Manning and if they (the Army) are unhappy with Manning('s) current status, then someone in the Army needs to take custody of him or relive (sic) us of the responsibility of his welfare." He will further testify that he "reiterated our concern (the marines) that if something goes wrong, there is not a single Army person that would be held responsible or found to be accountable as long as he stays with us." LtCol. Greer will testify that he was included on emails where LtCol. Wright, the then Head of Law Enforcement and Corrections Branch for Headquarters, U.S. Marine Corps, stated "to take measures that are consistent with suicide watch, but not officially place that person in a suicide watch status is inconsistent with the way we are supposed to do business."

- g) CPT John Haberland, john.haberland@us.army.mil, Regimental Judge Advocate, 201 Jackson Ave, Fort Myer, VA 22003, (703) 696-3150. He will testify that he acted as the conduit between the Army and Marines regarding the confinement of PFC Manning. Specifically, he will testify that he collected information in order to address a possible Article 13 motion by the Defense, and coordinated responses to the Defense regarding the confinement restrictions imposed upon PFC Manning. CPT Haberland will testify about how the Army knew of the manner in which PFC Manning was being held at MCBQ; the multiple complaints by PFC Manning's civilian counsel regarding the custody conditions; PFC Manning's multiple Article 138 complaints; and PFC Manning RCM 305(g) request to COL Coffman to either remove him from pretrial confinement or direct his removal from POI.

2. The Defense requests that the Government stipulate to the relevance and necessity of its own witnesses for the purposes of RCM 703. Thus, the Defense hereby incorporates and adopts the following witnesses identified by the United States as Government witnesses on 14 August 2012:

- a) COL Carl Coffman, United States Forces-Afghanistan, carl.coffman@us.army.mil;
- b) CW05 Abel Galaviz, Security and Law Enforcement Branch, Security Division, Corrections Section, Arlington, VA, 22204, (703) 604-4503;
- c) CW04 James Averhart, Navy Consolidated Brig Cheasapeake, Cheasapeake, VA, 23222, (707) 421-8672;
- d) CW02 Denise Barnes, Deputy Command Inspector General, Marine Corps Base Quantico (MCBQ), Quantico, VA 22134, (703) 432-0049;
- e) MSgt Craig Blenis, Security Battalion, Camp Pendleton, CA, 92055, (760) 725-8567;
- f) MSgt Brian Papakie, HQMC, Arlington, VA, 22204, (703) 604-4129; and
- g) GySgt William Fuller, Headquarters Marine Corps (HQMC), Arlington, VA, 22204, (703) 604-4138;

3. The Defense reserves the right to supplement this witness list should it be necessary to do so. If the Defense submits any additional request for witnesses, it will do so in a timely manner.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA )

v. )

Prosecution Witness List

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

14 August 2012

The United States may call the following witnesses to testify at the Article 13 motion hearing of the above-captioned court-martial:

1. CWO4 James Averhart, Navy Consolidated Brig Chesapeake, Chesapeake, VA, 23322, (707) 421-8672
2. CWO2 Denise Barnes, Deputy Command Inspector General, Marine Corps Base Quantico (MCBQ), Quantico, VA, 22134, (703) 432-0049
3. MSgt Craig Blenis, Security Battalion, Camp Pendleton, CA, 92055, (760) 725-8567
4. CPT Joseph Casamatta, 2d Battalion, 346th Regiment, Camp Shelby, MS, 39407, (703) 399-1730
5. Col (R) Daniel Choike (currently on terminal leave), Technology Associates, McLean, VA, 22101, daniel.choike@taic.net
6. LCpl Jonathan Cline, Headquarters Security Battalion, Quantico, VA, 22134, (781) 956-2406
7. COL Carl Coffman, United States Forces-Afghanistan, carl.coffman@us.army.mil
8. GySgt William Fuller, Headquarters Marine Corps (HQMC), Arlington, VA, 22204, (703) 604-4138
9. CWO5 Abel Galaviz, Security and Law Enforcement Branch, Security Division, Corrections Section, Arlington, VA, 22204, (703) 604-4503
10. SSG Ryan Jordan, United States Army Recruiting Command, ryan.jordan4@us.army.mil
11. MSgt Brian Papakie, HQMC, Arlington, VA, 22204, (703) 604-4129
12. CAPT (R) Jonathan Richardson (currently on terminal leave), Oceanside, CA, 92049, (760) 725-1555
13. LTC Robert Russell, Joint Task Force Guantanamo Bay (JTF-GTMO) (will be departing for JTF-GTMO on or about 22 September 2012), robert.k.russell.mil@health.mil

14. Mr. Joshua Tankersly, Gray Court, SC, 29645, (864) 684-9840
15. GM1 Terrance Webb, Navy Munitions Command, CONUS East Division, Detachment Sewells Point, Norfolk, VA, 23513, (757) 443-0800
16. LCDR Eve Weber, Naval Academy Annapolis, Annapolis, MD, 21402, eve.weber@med.navy.mil
17. ISG Bruce Williams, Headquarters and Headquarters Company, United States Army Garrison, Joint Base Myer-Henderson Hall, VA, 22211, (703) 696-3409

The United States reserves the right to supplement this witness list based on the defense's supplemental witness list, and supplemental motion.

If the defense intends to produce a witness who is listed above, the defense must provide a separate, appropriate request for that witness in accordance with Rule for Courts-Martial (RCM) 703 and the standard articulated in United States v. Rockwood, 52 M.J. 98, 105 (1999) that a witness request include a "synopsis of expected testimony," not merely a list of topics to be covered. If necessary for a particular witness employed by the United States Government, the defense shall also comply with 5 U.S.C. § 301 and Touhy v. Ragen, 340 U.S. 462 (1951).

ALEXANDER VON ELTEN  
CPT, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 14 August 2012.

ALEXANDER VON ELTEN  
CPT, JA  
Trial Counsel



UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Government Response  
to Defense Witness Request:  
Article 13**

**22 August 2012**

The Government reviewed the Defense witness request dated 15 August 2012 (Defense Request). Pursuant to Rule for Courts-Martial (RCM) 703(b)(1), the United States makes the following determinations regarding Defense requested Article 13 witnesses:

1. LtGen George Flynn: The United States denies production of LtGen Flynn. The Defense's proffered testimony of LtGen Flynn is not relevant and necessary under RCM 703(b)(1). LtGen Flynn was the commanding general of the Marine Corps Combat Development Command, located at Marine Corps Base Quantico (MCBQ). LtGen Flynn was the commanding officer for Col Choike, who was the commander of MCBQ, and Col Choike was the commanding officer of Col Oltman. Col Choike's and Col Oltman's proffered testimony makes LtGen Flynn's testimony cumulative and unnecessary. The Defense has not offered any evidence to support its theory that LtGen Flynn issued any orders regarding the accused's classification and status. For example, the email cited by the Defense is LtGen Flynn's response to an article in the New York Times and simply describes LtGen Flynn's concern for the accused's safety. Additionally, Col Choike, Col Oltman, CWO4 Averhart, and CWO2 Barnes will testify that LtGen Flynn was not involved with the day-to-day issues regarding the accused nor did LtGen Flynn give any instructions concerning the accused's classification and status.
2. Col Christopher Miner: The United States denies production of Col Miner. The Defense's proffered testimony of Col Miner is not relevant and necessary under RCM 703(b)(1). Col Miner was the staff judge advocate (SJA) to LtGen Flynn. In his role as SJA, Col Miner was carbon copied on emails and provided legal counsel to LtGen Flynn. Col Miner is irrelevant because he did not make any determinations with regard to the accused's classification and status. Col Choike, Col Oltman, CWO4 Averhart, and CWO2 Barnes will testify regarding the limited extent of LtGen Flynn's involvement, thereby making Col Miner's testimony cumulative and unnecessary.
3. Col Daniel Choike: The United States will produce Col Choike.
4. CDR Han Bui: The United States will produce CDR Bui. CDR Bui provided medical care to the accused.
5. CAPT Mary Neill: The United States denies production of CAPT Neill. The Defense's proffered testimony of CAPT Neill is not relevant and necessary under RCM 703(b)(1). CAPT Neill is a dentist and was the commander of the Naval Health Clinic at MCBQ. CAPT Neill's testimony is irrelevant because she did not provide psychiatric or medical care to the accused. CAPT Neill did not proffer an opinion on the accused's POI status or classification. During a

APPELLATE EXHIBIT 24  
PAGE REFERENCED:  
PAGE \_\_\_ OF \_\_\_ PAGES

telephonic interview with the prosecution in response to the Defense Request, CAPT Neill stated that she did not recall Col Oltman blaming CAPT Hocker for failing to identify the individual who committed suicide in January 2010 as a suicide risk. Col Oltman will be a witness and can testify about his own thoughts regarding CAPT Hocker's recommendations, thereby making CAPT Neill's testimony cumulative and unnecessary. CAPT Neill stated that she suggested the parties gather to discuss the process of determining the accused's status and classification, but she did not offer opinions regarding the actual decisions of what the accused's status and classification should have been.

6. LtCol Christopher Greer: The United States denies production of LtCol Greer. LtCol Greer was the SJA to Col Choike and Col Oltman. The Defense's proffered testimony of LtCol Greer is not relevant and necessary under RCM 703(b)(1). The Defense has not presented any evidence demonstrating that LtCol Greer possesses a unique perspective. The Defense proffers testimony from both Col Oltman and CAPT Hocker that they will testify about their own statements and what other statements each heard during meetings; therefore, LtCol Greer's testimony is cumulative and unnecessary. LtCol Greer's testimony is also irrelevant because LtCol Greer did not make any determinations regarding the accused's classification and status during the accused's confinement.

7. CPT John Haberland: The United States denies production of CPT Haberland. CPT Haberland was a member of the prosecution team during the accused's confinement at the Brig at MCBQ. CPT Haberland's comments and writings are work product. Therefore, CPT Haberland's communication and testimony are privileged. RCM 701(f); *see also United States v. Vanderwier*, 25 M.J. 263, 269 (C.M.A. 1987) ("Even though liberal, discovery in the military does not 'justify unwarranted inquiries into the files and the mental impressions of an attorney.'" (quoting *Hickman v. Taylor*, 329 U.S. 495, 510 (1947))).

The United States does not stipulate to the relevance and necessity of its witnesses for the purposes of RCM 703. The United States denies production of the following individuals: COL Carl Coffman, CWO5 Abel Galaviz, CWO4 James Averhart, CWO2 Denise Barnes, MSgt Craig Blenis, MSgt Brian Papakie, and GySgt William Fuller. The Defense's request fails to meet the *United States v. Rockwood*, 52 M.J. 98, 105 (C.A.A.F. 1999), and the RCM 703(c)(2)(B)(i) standard that a witness request include a "synopsis of expected testimony." The Defense's request does not provide an adequate description of the proffered testimony for these witnesses under RCM 703(c)(2)(B)(i). The United States will reconsider this request should the Defense proffer an adequate description demonstrating the relevance and necessity to the Defense's case of each witness's expected testimony.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 22 August 2012.

A handwritten signature in black ink, consisting of a stylized capital 'A' with a vertical line through it, enclosed within a loop.

ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

**DEFENSE MOTION TO  
COMPEL PRODUCTION  
OF WITNESSES FOR  
ARTICLE 13 MOTION**

DATED: 24 August 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (RCM) 703(b)(1) requests this Court to compel production of the below listed witnesses .

BACKGROUND

2. The Defense requests that the Court consider the background facts provided in Appellate Exhibit 206 and in the Defense Supplemental Article 13 Motion filed on 24 August 2012.

3. The Government provided 84 emails to the Defense on 26 July 2012. After having an opportunity to review these emails, the Defense identified additional witnesses for the Article 13 motion. The Defense obtained the latest available contact information for each of the witnesses on either Army Knowledge Online (AKO) or the Joint Enterprise Directory Services (JEDS). However, due to retirements, deployments, or just outdated information on AKO or JEDS the Defense was not able to coordinate interviews of some of the witnesses.

4. On 14 August 2012, the Government provided the Defense with its witness list for the Article 13 motion. The Government listed 17 witnesses that it intended to call for the purposes of the motion.

5. On 15 August 2012, the Defense filed its supplemental Article 13 witness list. By that point, the Defense had narrowed its witness list to 14 additional witnesses. Seven of the identified witnesses were also on the Government's witness list. As such, the Defense listed these witnesses by name and requested that the Government stipulate to their obvious relevance and necessity given the fact the Government planned to call them as well.

6. For the other seven witnesses not on the Government's witness list, the Defense provided a synopsis of their expected testimony under RCM 703(c)(2)(B)(i). The proffer clearly demonstrated the relevance and necessity for each of the following requested witnesses:

FILED IN 242  
PAGE 1 OF 1

- a) LtGen. George J. Flynn;
- b) Col. Christopher Miner;
- c) Col. (R) Daniel Choike;
- d) CDR Han Bui;
- e) Capt. Mary Neill;
- f) LtCol. Christopher Greer; and
- g) CPT John Haberland;

7. On 22 August 2012, the Government provided its response to the additional requested witnesses by the Defense. The Government denied production of LtGen. Flynn, Col. Miner, Capt. Neill, LtCol. Greer, and CPT Haberland. Additionally, the Government refused to stipulate to the relevance and necessity of its own listed witnesses for the purposes of RCM 703. As such, the Government denied the production of COL Carl Coffman, CWO5 Abel Galaviz, CWO4 James Averhart, CWO2 Denise Barnes, MSgt Craig Blenis, MSgt Brian Papakie, and GySgt William Fuller.

### ARGUMENT

#### **A. The Government is Acting in Bad Faith in Contesting the Relevance and Necessity of Its Own Witnesses**

8. The Government is once again proceeding in bad faith in contesting the relevance and necessity of numerous facially relevant witnesses. The Defense has never heard of a scenario where the Government has contested the relevance and necessity of *its own witnesses*. How can it be that a witness is relevant and necessary for the Government, but not equally relevant and necessary for the Defense? The Government opposes production of these witnesses, apparently because it believes the Defense did not comply with RCM 703(c)(2)(B)(i) and *United States v. Rockwood*, 52 M.J. 98 (C.A.A.F. 1999). RCM 703(c)(2) is intended to be administrative in nature such that the Government can arrange to actually contact these witnesses and bring them to court. As stated in the Analysis to RCM 703:

[T]he trial counsel is responsible for the administrative aspects of production of witnesses. Thus, . . . the defense submits its list of witnesses to the trial counsel so that the latter can arrange for their production. The trial counsel stands in a position similar to a civilian clerk of court for this purpose. Because most defense requests for witnesses are uncontested, judicial economy is served by routing the list directly to the trial counsel, rather than to the military judge first. This also allows the trial counsel to consider such alternatives as offering to stipulate or take a deposition, or recommending to the convening authority that a charge be withdrawn . . . . Further, it allows arrangements to be made in a more timely manner, since the trial counsel is usually more readily available than the military judge. *Only if there is a genuine dispute as to whether a witness must be produced is the issue presented to the military judge by way of a motion.*

Drafters' Analysis, *Manual for Courts-Martial, United States (MCM)*, A21-36 (2008 ed.)(emphasis added). Is the Government truly saying that there is a "genuine dispute" as to whether witnesses that the Government itself plans to call must be produced? As with so many other issues in this case, the lack of good faith on the part of the Government is troubling.

9. The Defense believes that the witnesses on the Government's witness list are relevant and necessary for painfully obvious reasons:

- a) CWO4 James Averhart and CWO4 Denise Barnes. Both were the Officers in Charge of the Brig during the relevant time period. Both (at least in theory) made the custodial classification determinations pertaining to PFC Manning. Both will testify regarding their classification determinations, their disdain for, and questioning of, medical opinions, and their knowledge of LtGen. Flynn's involvement in the case. Both will testify about the specific instances that PFC Manning was placed on Suicide Risk or where his special handling instructions were increased.
- b) COL Carl Coffman. COL Coffman was the Special Court-Martial Convening Authority. He will testify about what he knew about PFC Manning's confinement conditions and why he did not ask Quantico officials to remove PFC Manning from POI. He will also testify about whether he knew of LtGen. Flynn's involvement in the case.
- c) MSgt Craig Blenis, MSgt Brian Papakie, and GySgt William Fuller. All these individuals sat on PFC Manning's C&A Board and will testify why they made recommendations to retain PFC Manning in MAX and on POI despite doctors' recommendations to the contrary. All these individuals will testify that they knew about LtGen Flynn's involvement in the case. MSgt Papakie will testify about his homophobic comment about PFC Manning's "panties." MSgt Blenis will testify why he made the comment to the effect of "We felt like being dicks." GySgt Fuller will testify about the harassment of PFC Manning during recreation call on 18 January 2011.
- d) CWO5 Abel Galaviz. He will testify about his "independent" investigation at the behest of Col. Choike. He will also testify that he was involved in PFC Manning's confinement since he arrived at Quantico and was copied on numerous emails prior to being assigned as an "independent" investigator as part of the Article 138 Complaint.

#### **B. The Additional Witnesses Denied By the Government Are Relevant and Necessary**

10. The Defense is entitled to production of witnesses whose testimony "would be relevant and necessary" to a matter in issue. RCM 703(b)(1). In determining relevance of the witness, a court must turn to the Military Rules of Evidence. See, e.g., *United States v. Breeding*, 44 M.J. 345, 351 (C.A.A.F. 1996). A witness is necessary when the witness is not cumulative, and when the witness would contribute to a party's presentation of the case in some positive way on a matter in issue." *United States v. Credit*, 8 M.J. 190, 193 (CMA 1980); see also *United States v. Williams*, 3 M.J. 239 (C.M.A. 1977).

11. The Defense requests production of LtGen. George Flynn, Capt. Mary Neill, LtCol. Christopher Greer, Col. Christopher Miner, and CPT John Haberland.

12. LtGen. George Flynn. In its original witness request, the Defense stated the relevance and necessity of LtGen. Flynn's testimony:

LtGen. George J. Flynn, george.j.flynn@usmc.mil, Director for Joint Force Development, The Joint Staff J-7. LtGen. Flynn is the former Commanding General of Marine Corps Combat Development Command. As the Commanding General, he was the senior rater for Col. Daniel Choike, the former Marine Corps Base Quantico (MCBQ) Commander and Col. Robert Oltman, the former MCBQ Security Battalion Commander. LtGen. Flynn will testify about requiring the Quantico Brig to report to him, for his approval, regarding any change in PFC Manning's handling instructions or assignment status. LtGen. Flynn will testify that prior to any final action taken place with changing PFC Manning's custody status, he wanted to be able to determine the political impact, media interest, legal ramifications, and senior leadership reactions. LtGen. Flynn will testify that he received frequent reports, at least once a week, on PFC Manning and his custody status. LtGen. Flynn will testify that he first made inquiries into PFC Manning within a week of his arrival at MCBQ. He will testify that he was concerned about the suicide risk of PFC Manning. He will testify that the Brig had a suicide on 31 January 2010. Based upon the previous suicide he directed Col. Choike and Col. Oltman to impress "upon all who come in contact with Pvt. Manning the absolute necessity of keeping a close watch on him... His [PFC Manning] life has completely fallen apart which makes him a strong candidate (from my perspective) to take his life." Finally, LtGen. Flynn will recount how he became involved in the day to day issues regarding PFC Manning.

13. The Government contests the relevance and necessity of LtGen. Flynn's testimony largely by attempting to mislead the Court. The Government writes:

Col Choike's and Col Oltman's proffered testimony makes LtGen Flynn's testimony cumulative and unnecessary. The Defense has not offered any evidence to support its theory that LtGen Flynn issued any orders regarding the accused's classification and status. For example, the email cited by the Defense is LtGen Flynn's response to an article in the New York Times and simply describes LtGen Flynn's concern for the accused's safety. Additionally, Col Choike, Col Oltman, CWO4 Averhart, and CWO2 Barnes will testify that LtGen Flynn was not involved with the day-to-day issues regarding the accused nor did LtGen Flynn give any instructions concerning the accused's classification and status. *See* Government Response to Defense Witness Request: Article 13, p. 1.

14. The Defense does not understand the Government's "cumulative" argument. The Government states that Col. Choike, Col. Oltman, CWO4 Averhart and CWO2 Barnes will all testify about LtGen. Flynn's involvement in PFC Manning's custody status. *Id.* It seems obvious that LtGen. Flynn can best speak to LtGen. Flynn's involvement in the case – and the other witnesses will be used to either corroborate or discount this testimony. The Defense's

position is that PFC Manning's custody status in this case was ultimately determined by LtGen. Flynn. Everyone below him in the chain of command was putting LtGen. Flynn's guidance into effect. How is it, then, that LtGen. Flynn's testimony is cumulative?

15. Further, the Government's statement that the Defense "has not offered any evidence to support its theory that LtGen. Flynn issued any orders regarding the accused's classification status" is ludicrous. In an email from Col. Choike to Col. Oltman (which was provided to the Defense by the Government), Col. Choike clearly states:

You and I supporting/concurring with the Brig OIC's decisions that change handling instructions or assignment status, without passing that info to CG MCCDC [LtGen. Flynn] for consideration, is no longer acceptable. We/you are not going to get anything in writing from CG MCCDC [LtGen. Flynn] if he rejects/modifies a recommendation. Memo's for the record can be discussed more between you and I, in an effort to address your concerns about proper documentation/file keeping.

Summary - #1 - yes adhere to the chain of command, and hopefully you understand why that didn't happen right now. #2 Yes - recommendations forwarded to me for discussion and concurrence and then recommendation forwarded to CG, MCCDC [LtGen. Flynn] before implementation. I will not blindly forward a recommendation to the CG, instead I'll discuss it with you so you will know exactly what I forward. #3 Non-concurrence in writing - we need to discuss and determine the best way to document decision/final actions for the record. CG [LtGen. Flynn] wants to be able to determine political impact, media interest, legal ramifications, and senior leadership reactions, and can't do so without him being in the loop upfront.

See Attachment A to Defense Supplemental Article 13 Motion, Bates Number 00449914 through 00449915. It is abundantly clear from this one email alone that LtGen. Flynn was the one who was "calling the shots." Decisions that "change handling instructions or assignment status" were to be made ultimately by LtGen. Flynn. LtGen. Flynn, in making these determinations, wanted to be able to "determine the political impact, media interest, legal ramifications, and senior leadership reactions" about anything involving PFC Manning's confinement status. *Id.* In light of just this one email (not to mention the others that the Government has provided), it is a flat out falsehood to say that "LtGen Flynn did not give any instructions concerning the accused's classification and status." The Government also contests that LtGen Flynn was involved in day-to-day issues regarding the accused. Apparently, the Government must have missed the email to LtGen. Flynn explaining that Defense counsel had called the Brig after hours, or the email where LtGen. Flynn asked whether PFC Manning's visitors who had been denied entrance to Quantico had been called a cab. See Attachment A to Defense Supplemental Article 13 Motion, Bates Number 0044933-36.

16. It is obvious why the Government is making this feeble attempt to contest the relevance and necessity of LtGen. Flynn's testimony – it is rather embarrassing to have to call a three-star general and explain why he was giving guidance to those in his chain of command that he would



ultimately call the shots when it came to PFC Manning. However, in light of these emails, there is no witness who is *more* relevant and necessary for production than LtGen. Flynn.

17. Capt. Mary Neill. Capt. Neill is the former commander of the Naval Health Clinic at MCBQ. She will testify that Col. Choike ordered her to provide him with a weekly update on PFC Manning. She will testify that she complied with this order by providing at least weekly reports to Col. Choike. Capt. Neill will testify that the Brig psychiatrists would provide her with a weekly report that she would then add to for the benefit of Col. Choike and LtGen. Flynn. Within the report, she would discuss the results of the behavioral health visits, the recommendation of the Brig psychiatrists, the nature of PFC Manning's custody status, and PFC Manning's overall affect and mood. She will testify that she was aware of the Brig psychiatrists, Capt. William Hoyer and COL Robert Malone's consistent recommendations to remove PFC Manning from POI watch. Despite their frequent recommendations, PFC Manning was never removed from POI. Capt. Neill will testify that Col. Oltman had come to her to express his loss of trust in the recommendations of Capt. Hoyer. She will testify that Col. Oltman blamed Capt. Hoyer for failing to identify the individual who committed suicide in January of 2010 as a potential suicide risk. She will testify that she was aware that the Brig had displayed significant concern and was very anxious about the high level of visibility regarding PFC Manning and the associated risks. Capt. Neill believed that the Brig staff would benefit from having some of their questions and concerns addressed by her medical staff. She will also testify that she informed Col. Choike and Col. Oltman that it was her opinion that the continuation of POI was not detrimental to PFC Manning. Capt. Neill will testify that she was also aware of Capt. Hoyer's repeated requests for the Brig to allow PFC Manning the opportunity to exercise in his cell. She will testify that Capt. Hoyer had noted a decline in the physical conditioning of PFC Manning due to his limited opportunities to be out of his cell. She also will testify that she took it upon herself to have a face to face meeting with the Capt. Brian Moore, the former Defense forensic psychiatrist expert, to inform him that his access to PFC Manning was only through the defense counsel channels, and that since his appointment to the Defense team, he was no longer part of behavioral health provider team for PFC Manning.

18. The Government has denied production of Capt. Neill on the following basis:

The United States denies production of CAPT Neill. The Defense's proffered testimony of CAPT Neill is not relevant and necessary under RCM 703(b)(1). CAPT Neill is a dentist and was the commander of the Naval Health Clinic at MCBQ. CAPT Neill's testimony is irrelevant because she did not provide psychiatric or medical care to the accused. CAPT Neill did not proffer an opinion on the accused's POI status or classification. During a telephonic interview with the prosecution in response to the Defense Request, CAPT Neill stated that she did not recall Col Oltman blaming CAPT Hoyer for failing to identify the individual who committed suicide in January 2010 as a suicide risk. Col Oltman will be a witness and can testify about his own thoughts regarding CAPT Hoyer's recommendations, thereby making CAPT Neill's testimony cumulative and unnecessary. CAPT Neill stated that she suggested the parties gather to discuss the process of determining the accused's status and classification, but she did not offer opinions regarding the actual decisions of what the accused's status and

classification should have been. *See* Government Response to Defense Witness Request: Article 13, p. 1-2.

19. It is not true that Capt. Neill did not “proffer an opinion on the accused’s POI status.” Capt. Neill was tasked with taking information from Capt. Hoctor and Col. Malone and passing it up the food chain to Col. Oltman (where ultimately it was passed onto Col. Choike and LtGen. Flynn). The fact that Capt. Neill was a dentist raises questions as to why she was entrusted to be the “broken telephone” conduit. It is indeed strange that psychiatric opinions are filtered through a dentist up the chain of command. In one instance, on 2 February 2011, after Capt. Neill forwarded Col. Malone’s recommendation to remove PFC Manning to Col. Oltman, Col. Oltman writes, “The Dr. Recommends removal from POI but stats [sic] that the risks and benefits of continued POI are not detrimental ... or at least that’s how I read what he wrote.” *See* Attachment A to Defense Supplemental Article 13 Motion, Bates Number 00449840. Then Capt Neill weighs in, “Concur that Psych review states that remaining in continuation of POI is NOT detrimental to detainee.” *Id.* Why is Capt. Neill, a dentist, weighing in on how she interprets the doctor’s recommendation? Why is Capt. Neill, a dentist, tasked with the role of keeping Col. Oltman in the loop?

20. LtCol. Christopher Greer. LtCol. Greer will testify that he was present for the meeting where Col. Oltman stated that PFC Manning would remain in his current status Maximum Custody and POI unless and until he received instructions from higher authority to the contrary. LtCol. Greer will testify that he did not attempt to intervene or correct Col. Olman when he told Capt. Hoctor something to the effect of “I will not have anything happen to Manning on my watch. So, nothing is going to change in his custody status. He won’t be able to hurt himself and he won’t be able to get away, and our way of making sure of that is that is he will remain on Maximum Custody and POI indefinitely.” LtCol. Greer will testify that Capt. Hoctor became upset and expressed his concern about holding PFC Manning in POI when there was no behavioral health justification for such a status. He will testify that Capt. Hoctor did not support the POI status, but was told that his recommendation was just a part of the overall classification assessment. He will testify that Col. Oltman told Capt. Hoctor that he should just make his recommendations and that they (the confinement facility) would do what they wanted to do. LtCol. Greer will also testify that he provided regular updates to Col. Choike, Col. Oltman, and LtGen. Flynn’s SJA (Col. Christopher Miner) about PFC Manning. Finally, LtCol. Greer will testify that he was aware of a request by the Defense to the Convening Authority, COL Coffman, to remove PFC Manning from POI. He will testify that he informed Col. Choike and Col. Oltman to “stand by for heavy rolls if the CA decides to request the Base commander to review and consider removing Manning’s POI status.” He will also testify that he informed the Army that “unless you want to run our Brig, I think you undercut your own legal position if you actually recommend that the POI status be removed. We are the jailors, either you trust us or you don’t. If you don’t, then move him.” LtCol. Greer also will testify that he informed the prosecution that “we (the marines) have the day to day responsibility for Manning and if they (the Army) are unhappy with Manning(’s) current status, then someone in the Army needs to take custody of him or relive (sic) us of the responsibility of his welfare.” He will further testify that he “reiterated our concern (the marines) that if something goes wrong, there is not a single Army person that would be held responsible or found to be accountable as long as he stays with us.” LtCol. Greer will testify that he was included on emails where LtCol. Troy Wright, the Head of Law Enforcement and Corrections Branch for Headquarters, U.S. Marine Corps, stated

“to take measures that are consistent with suicide watch, but not officially place that person in a suicide watch status is inconsistent with the way we are supposed to do business.”

21. The Government resists producing LtCol. Greer on the following basis:

The Defense has not presented any evidence demonstrating that LtCol Greer possesses a unique perspective. The Defense proffers testimony from both Col Oltman and CAPT Hoyer that they will testify about their own statements and what other statements each heard during meetings; therefore, LtCol Greer’s testimony is cumulative and unnecessary. LtCol Greer’s testimony is also irrelevant because LtCol Greer did not make any determinations regarding the accused’s classification and status during the accused’s confinement. *See* Government Response to Defense Witness Request: Article 13, p. 2.

22. The test is not whether LtCol. Greer possesses a “unique perspective” – the test is whether his testimony would contribute to the Defense’s presentation of the case in some positive way on a matter in issue.” *United States v. Credit*, 8 M.J. 190, 193 (CMA 1980); *see also United States v. Williams*, 3 M.J. 239 (C.M.A. 1977). The Defense submits that LtCol. Greer will corroborate Dr. Hoyer’s recollection that he very clearly and emphatically stated that PFC Manning should not be on POI from a psychiatric perspective. He will also testify that he relayed the contents of this meeting to trial counsel (presumably MAJ Fein), such that MAJ Fein was also aware that POI was not recommended from a psychiatric perspective and was on notice of Article 13 issues. LtCol. Greer will also testify that he wrote an email recommending that the Army not make a fuss about these issues lest it be “prepared for heavy rolls.” *See* Attachment A to Defense Supplemental Article 13 Motion, Bates Number 00449938-9. LtCol. Greer will also testify that he knew about LtGen. Flynn’s involvement from Day 1 in PFC Manning’s case.

23. Col. Christopher Miner. He will testify that he was the SJA for LtGen. Flynn. He will testify that he received regular briefs from LtCol. Greer, Col. Oltman, and Col. Choike regarding PFC Manning. Based upon the briefs he received from others, Col. Miner would provide advice to LtGen. Flynn regarding PFC Manning. Col. Miner was included upon emails where Col. Oltman informed the command that the Brig OIC, CWO4 Averhart, was holding PFC Manning on Suicide Risk (SR) after the mental health professionals had recommended his status be changed from SR to Prevention of Injury (POI). Col. Miner will testify that he was aware of the level of involvement by LtGen. Flynn in the custody status of PFC Manning.

24. The Government resists producing Col. Miner because it believes his testimony is cumulative and unnecessary and that others will testify regarding the involvement of LtGen. Flynn. *See* Government Response to Defense Witness Request: Article 13, p. 2. Col. Miner is neither cumulative nor unnecessary. He is clearly involved in the discussions concerning PFC Manning’s custody status and the guidance provided by LtGen. Flynn’s to his subordinates. As such, Col. Miner is a relevant and necessary witness.

25. CPT John Haberland. He will testify that he acted as the conduit between the Army and Marines regarding the confinement of PFC Manning. Specifically, he will testify that he collected information in order to address a possible Article 13 motion by the Defense, and

coordinated responses to the Defense regarding the confinement restrictions imposed upon PFC Manning. CPT Haberland will testify about how the Army knew of the manner in which PFC Manning was being held at MCBQ; the multiple complaints by PFC Manning's civilian counsel regarding the custody conditions; PFC Manning's multiple Article 138 complaints; and PFC Manning RCM 305(g) request to COL Coffman to either remove him from pretrial confinement or direct his removal from POI.

26. The Government resists producing CPT Haberland on the basis that "CPT Haberland was a member of the prosecution team during the accused's confinement at the Brig at MCBQ. CPT Haberland's comments and writing are work product." *See* Government Response to Defense Witness Request: Article 13, p. 2. The Government has provided the Defense with emails written by CPT Haberland. Thus, to the extent that privilege exists, it has been waived with respect to these emails. Moreover, the Defense will not be inquiring into attorney work product. Instead, the Defense will inquire about the extent of the Army's knowledge of PFC Manning's confinement conditions.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE MOTION TO  
COMPEL DISCOVERY #3**

17 August 2012

RELIEF SOUGHT

1. In accordance with the Rules for Courts Martial (RCM) 701(a)(2) and 905(b)(4), Manual for Courts-Martial (MCM), United States, 2008; Article 46, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 846; and the Fifth and Sixth Amendments to the United States Constitution, the Defense respectfully requests that the Court compel the requested discovery. Specifically, the Defense requests that the Court order the Government to produce the remaining 1,290 emails that it obtained from Marine Corps Base Quantico (MCBQ) regarding the confinement conditions of PFC Manning.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. RCM 905(c)(2)(A). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

EVIDENCE

3. The Defense does not request any witnesses be produced for this motion. The Defense requests that this Court consider the following evidence in support of this motion:

- a) Attachment A (Government's Preservation Request, dated 28 April 2011);
- b) Attachment B (Response by Quantico indicating all electronic correspondence has been provided to the trial counsel, dated 20 December 2011);
- c) Attachment C (Government Discovery Response, dated 14 August 2012);
- d) Attachment D (Email from MAJ Ashden Fein, dated 26 July 2012);
- e) Attachment E (Email from MAJ Ashden Fein, dated 27 July 2012); and
- f) Attachment F (Email from MAJ Ashden Fein, dated 14 August 2012).

FACTS

4. On 28 April 2011, the Government submitted a "request for prudential search and preservation of information" to Col. Daniel Choike, the Commander of Quantico. See Attachment A. The document submitted by MAJ Fein requested Col. Choike to "take any and

all reasonable and necessary steps to preserve any information held by your command which concerns or references PFC Manning” and secondly “that your command conduct a thorough and comprehensive search of its records for information which relates to PFC Manning’s confinement at the Quantico Brig.” *Id.* In August of 2011, the Government began receiving documentation responsive to its preservation request. *See* Attachment C.

5. On 20 December 2011, LtCol. Christopher M. Greer, the Staff Judge Advocate for Col. Oltman, confirmed that “all relevant electronic correspondence, electronic files and hard copy documentary evidence regarding the confinement of PFC Manning in the possession of Marine Corp [B]ase Quantico official[s] have been provided. Trial counsel were (sic) permitted to view and copy all relevant files maintained by the Quantico Pretrial Confinement Facility.” *See* Attachment B.

6. The Government began providing documentation related to PFC Manning’s confinement at Quantico in October of 2011. Based upon the volume of the information provided, the Defense believed that this was the full extent of the information the Government had from Quantico.

7. On 25 July 2012, almost a year after the Government first began receiving documentation from Quantico, and almost seven months after receiving the last of the Quantico documentation, the Government started reviewing the emails that it had received from Quantico. *See* Attachment C. According to the Government, it started reviewing these emails “in preparation for the defense Article 13 motion.” *Id.* 4. The Article 13 motion, however, had been on the case calendar since this case was referred. The established deadline for the Defense to file the Article 13 motion was 27 July 2012. Additionally, the Defense had already advised the Government that the Article 13 motion would be a very lengthy and involved motion, totaling over 100 pages. In fact, the case calendar had accommodated the Government’s request for an additional week to respond to the motion due to the anticipated length of the motion.

8. Once the Government elected to review the Quantico documentation, it reviewed a total of 1,374 emails on 25 and 26 July 2012. *Id.*, *see also*, Attachment F. On 26 July 2012, the Government selected 84 emails that it believed were “obviously material to the preparation of the defense” and produced them to the Defense. *See* Attachment D.

9. On 27 July 2012, the Defense notified the Court that MAJ Fein had sent, at 2115 on 26 July 2012, 84 separate emails which depicted high level discussions at Quantico concerning PFC Manning’s custody status. The Court held an RCM 802 conference on 27 July 2012 to discuss the need for a continuance in the consideration of the Article 13 motion.

10. As a result of the Government’s late discovery, the Defense requested a continuance of the proceedings in order to review and incorporate information from the 84 emails into its Article 13 submissions; to interview (and re-interview) witnesses based on information contained therein; and to file a supplemental Article 13 witness list. On 1 August 2012, the Court granted the Defense’s request.

## ARGUMENT

11. The emails from Quantico are in the possession, custody, and control of the military and fall within RCM 701(a)(2). While the Government has turned over a small fraction of this material, 84 emails, it has failed to turn over any of the remaining 1,290 emails which are “regarding the confinement of PFC Manning” and were turned over by Quantico in response to MAJ Fein’s “prudential search and preservation” request. *See* Attachments A and B.

12. RCM 701(a)(2)(A) provides that, after service of charges, upon request of the Defense, the Government shall permit the Defense to inspect:

Any books, papers, documents, photographs, tangible objects, buildings, or places, or copies of portions thereof, *which are within the possession, custody, or control of military authorities*, and which are material to the preparation of the defense or are intended for use by the trial counsel as evidence in the prosecution case-in-chief at trial, or were obtained from or belong to the accused.

(emphasis supplied).

13. The Government has previously maintained that if an organization is subject to a military command, then this factor controls the determination of whether materials are within the possession, custody, or control of military authorities. *See* Appellate Exhibit XLIX. The Court has held that “the defense is entitled to disclosure of matters known to the trial counsel or in the possession of military authorities.” *See* Appellate Exhibit CXLVII, p. 4. Quantico is subject to a military command. Accordingly, the Government has an obligation to turn over documents that are material to the preparation of the defense.

14. As the Defense has argued before, the case law reaffirms that “material” under RCM 701(a)(2)(A) is not a difficult standard to satisfy. In *United States v. Cano*, 2004 WL 5863050 at \*3 (A. Crim. Ct. App. 2004), our superior court discussed the content of the “materiality” standard under R.C.M. 701(a)(2)(A):

In reviewing AE V in camera, the military judge said that he examined the records and AE III contained “everything . . . [he] thought was even remotely potentially helpful to the defense.” That would be a fair trial standard, but our examination finds a great deal more that should have been disclosed as “material to the preparation of the defense.” We caution trial judges who review such bodies of evidence in camera to do so with an eye and mind-set of a defense counsel at the beginning of case preparation. That is, not solely with a view to the presentation of evidence at trial, but to actually preparing to defend a client, so that the mandate of Article 46, UCMJ, is satisfied.

*See also United States v. Roberts*, 59 M.J. 323, 326 (C.A.A.F. 2004) (“The defense had a right to this information because it was relevant to SA M’s credibility and was therefore material to the preparation of the defense for purposes of the Government’s obligation to disclose under R.C.M.

701(a)(2)(A).”(emphasis added); *United States v. Webb*, 66 M.J. 89, 92 (C.A.A.F. 2008) (“[U]pon request of the defense, the trial counsel must permit the defense to inspect any documents within the custody, or control of military authorities that are ‘material to the preparation of the defense.’ R.C.M. 701(a)(2)(A). Thus, an accused’s right to discovery is not limited to evidence that would be known to be admissible at trial. It includes materials that would assist the defense in formulating a defense strategy.”).

15. On 8 December 2010, the Defense requested “[a]ny and all documents or observation notes by employees of the Quantico confinement facility relating to PFC Bradley Manning.” See Attachment E. In response to the Defense’s request, “the prosecution requested Quantico preserve all documentation and their emails.” *Id.*

16. In spite of receiving the 1,374 emails in response to its preservation request, the Government elected to permit these emails to collect dust in one of its file cabinets until two days before the Defense’s Article 13 motion was due. In defending its conduct, the Government will likely try to assert that it did not believe that an emails involving the Brig OIC and Brig personnel, or emails concerning PFC Manning’s confinement status were “documents or observations notes by employees of the Quantico confinement facility” within the meaning of the Defense’s discovery request. The Government will likely try to convince the Court that when it was reviewing the emails for *Giglio* and *Jencks* under RCM 914, it came across information that was obviously material to the preparation of the Defense and then turned the information over as soon as it was aware of its existence. Such a position is untenable. These emails are clearly “documents ... by employees of Quantico confinement facility relating to PFC Manning” and should have been produced a long time ago pursuant to the Defense’s discovery request. Indeed, the Government itself recognizes that these documents are discoverable under RCM 701(a)(2) as it indicates that these emails are “obviously material to the preparation of the defense.”

17. The Government was clearly aware of the fact that the Defense believed PFC Manning’s confinement conditions were unnecessarily onerous. PFC Manning had repeatedly requested to be removed from MAX and POI. Additionally, the Defense made numerous requests of the United States Army Staff Judge Advocate’s Office for the Military District of Washington to assist in removing PFC Manning from MAX and POI. In the fall of 2010, Mr. Coombs and MAJ Fein had several telephone conversations about the onerous conditions of PFC Manning’s confinement. MAJ Fein assured Mr. Coombs that he was looking into the issue and would view it as one of his highest priorities. See Defense Article 13 Motion, p. 47. PFC Manning was never taken off of MAX or POI status. And it is clear that MAJ Fein and the Government did not advocate for the rights of PFC Manning during this period despite repeated protestations from the Defense that PFC Manning was being subjected to illegal pretrial punishment.

18. Despite being aware of the impending Article 13 motion, the Government inexplicably chose to wait until two days before the filing of the Defense’s Article 13 motion before reviewing documents that it had been holding for close to a year. This conduct is either yet another example of that lack of due diligence on the Government’s part, or a conscious decision by the Government to gain a tactical advantage in the Article 13 motion.



19. The requested emails are clearly material to the preparation of the Defense. Their volume alone proves the extent of involvement by individuals outside of the Quantico Brig in the custody status and classification of PFC Manning. This undeniable fact clearly supports the Defense's argument that the decision to keep PFC Manning in MAX and POI for over nine months was not based upon a legitimate non-punitive basis. As such, all 1,374 emails are material to the preparation of the defense.

20. Moreover, it defies logic to believe that there are nearly 1,300 emails out there dealing with PFC Manning's confinement that are not somehow relevant and helpful to the preparation of the defense. With the exception (perhaps) of purely logistical issues,<sup>1</sup> it would seem that any email referencing PFC Manning's confinement is *per se* material to the preparation of the defense.<sup>2</sup>

21. One additional note: the Government has indicated that it has produced emails that are "obviously" material to the preparation of the Defense. This is *not* the appropriate standard. The Government must turn over all documents which are material to the preparation of the Defense – as in relevant and helpful. The Defense believes, based on the sheer volume of emails not produced, that the Government has not done so.

22. The Government has had anywhere from 7 months to over a year to review the 1,374 emails it received from Quantico. The Defense has not had equal access to this same information, or the ability to adequately factor this information into the Defense's Article 13 motion. The requested information is material to the preparation of the defense, and should be turned over immediately. To permit the Government to hold onto the remaining 1,290 emails will only reward its lack of due diligence, and result in the Defense being unable to demonstrate the full extent of the Article 13 violation.

### CONCLUSION

23. Under R.C.M. 701(a)(2), the Court should conclude that the remaining 1,290 emails being held by the Government from Quantico are within the "possession, custody, or control" of the Government and are material to the preparation of the Defense. The Court should compel the Government to produce these emails immediately to the Defense in order to avoid any additional requirement for a continuance of the Article 13 motion.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

---

<sup>1</sup> For instance, emails concerning PFC Manning's movement.

<sup>2</sup> The Government has proved that it is not adept at determining what is relevant or material to the preparation of the Defense. The Court should recall that the Government did not believe damage assessments were relevant. Further, the Government did not believe that the FBI investigation pertaining to PFC Manning was relevant. These examples show that the Government's incredibly narrow view of what is relevant is not in accord with what is *actually* relevant.

# ATTACHMENT A



REPLY TO  
ATTENTION OF

FOR OFFICIAL USE ONLY

DEPARTMENT OF THE ARMY  
U.S. ARMY MILITARY DISTRICT OF WASHINGTON  
210 A STREET  
FORT LESLEY J. MCNAIR, DC 20319-5013

ANIA-CL

28 April 2011

MEMORANDUM FOR Col Daniel Choike, Commander, Marine Corps Base Quantico

SUBJECT: Request for Prudential Search and Preservation of Information - U.S. v. PFC  
Bradley E. Manning

1. The U.S. Army Prosecutors in the above-referenced case ("prosecution") hereby make a two-fold request to the Marine Corps Base Quantico ("command"). First, the prosecution requests that your command take any and all reasonable and necessary steps to preserve any information held by your command which concerns or references **PFC Manning**. Secondly, the prosecution requests that your command conduct a thorough and comprehensive search of its records for information which relates to PFC Manning's confinement at the Quantico Brig.

2. This request is designed to allow the prosecutors to assess the totality of information available and held as records by your command. It is not intended to, nor should it be interpreted as, ascribing any legal relevance, including whether such information may be provided in discovery, to the information requested. The prosecutors require such materials immediately. In order to expedite this process, please provide the requested information that is "UNCLASSIFIED", "CONFIDENTIAL", or "SECRET" by 15 May 2011, on a CD or DVD. Any information classified "TOP SECRET" or controlled as "sensitive compartmented information", should be made available for inspection. We anticipate making future requests as the need arises, and specifically before the trial, if the case is referred to court-martial.

3. As stated above, the prosecution requests that you preserve all documents and information, including data stored on electronic media, pertaining to PFC Manning, whether or not such information is directly responsive. Furthermore, please take steps to preserve materials related to PFC Manning from any routine data destruction practices. If you are unsure whether certain materials should be preserved, please err on the side of caution and preserve the materials. Failure to preserve and retain any pertinent materials, electronic or otherwise, may result in sanctions against the United States, based on PFC Manning's rights under Article 46, UCMJ, the Rules for Courts-Martial, and applicable case law.

4. The point of contact for this request is the undersigned at (202) 685-1975, [ner.ediscovery@jthqnet.northcom.mil](mailto:ner.ediscovery@jthqnet.northcom.mil), or [ner.ediscovery@jthqnet.northcom.smil.mil](mailto:ner.ediscovery@jthqnet.northcom.smil.mil) (secure email).

ASSTJUDGE  
CPL USA  
Paul Choike

FOR OFFICIAL USE ONLY

# ATTACHMENT B




UNITED STATES MARINE CORPS  
OFFICE OF THE STAFF JUDGE ADVOCATE  
3250 CATLIN AVENUE  
MARINE CORPS BASE  
QUANTICO, VIRGINIA 22134

IN REPLY REFER TO:  
5800  
B052  
20 Dec 11

From: Staff Judge Advocate  
To: U.S Army Trial Counsel

Subj: DISCOVERY OF ELECTRONIC AND HARD COPY FILES ICO PRIVATE FIRST  
CLASS BRADLEY MANNING U.S. ARMY

1. Pursuant to trial counsel request, all relevant electronic correspondence, electronic files and hard copy documentary evidence regarding the confinement of PFC Manning in the possession of Marine Corps base Quantico official have been provided. Trial counsel were permitted to view and copy all relevant files maintained by the Quantico Pretrial Confinement Facility.

  
CHRIS GREEN  
LtCol, USMC

# ATTACHMENT C

UNITED STATES OF AMERICA )

v. )

Manning, Bradley F.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

Prosecution Response  
to Defense Discovery Request

14 August 2012

The prosecution hereby responds to the Defense Discovery Request dated 1 August 2012 as follows:

1. The memorandum e-mail document from the Government to Marine Corps Base Quantico (hereinafter "Quantico") requesting that they preserve and produce document and information pertaining to PFC Manning's confinement:

**RESPONSE:** On 8 March 2012, the prosecution provided this document as part of its Response to Defense Motion to Compel Discovery. See Enclosure 1 to Appellate Exhibit (AE) XVI.

2. The names of the individuals who the Government sent the Quantico preservation request to and the date which the Government made its request:

**RESPONSE:** On 8 March 2012, the prosecution provided this document as part of its Response to Defense Motion to Compel Discovery. See id. This document was sent through LtCol Christopher Greer, Staff Judge Advocate, Quantico to Col Daniel Chorke, Commander Quantico.

3. All documentation provided by these individuals in response to the Government's request, the date this information was provided, and the individuals who provided the requested information:

**RESPONSE:**

a. In August 2011, the prosecution began receiving documentation responsive to its preservation request and continued to work with Quantico to identify additional information. On 26 December 2011, LtCol Greer, confirmed that "all relevant electronic correspondence, electronic files and hard copy documentary evidence regarding the confinement of [the accused] in the possession of [Quantico] official have been provided." Enclosure 2 to AE XVI. On 8 March 2012, the prosecution provided the defense LtCol Greer's statement as part of its Response to Defense Motion to Compel Discovery. See id.

b. In August 2011, the prosecution started producing information it received from Quantico in response to the prosecution's preservation order, and by 6 December 2011, the prosecution

produced to the defense all documentation except two documents. On 27 July 2012, and in preparation for the defense Article 13 motion, the United States started receiving emails it received from Quantico, pursuant to the preservation request, for potential impeachment evidence or RCM 914 Jencks material. The United States identified eighty-four emails that were obviously material to the preparation of the defense, because they fell into these four categories: (1) statements by Brig officials describing their classification decisions, including the factors weighed; (2) statements discussing chain of command directives regarding the accused's confinement; (3) statements describing the condition of the accused's confinement, including descriptions of the accused; or (4) pertinent to the Court's prior Ruling, statements involving investigation, damage assessment, or mitigation measures. See AF CXI VII. The United States produced these emails on 26 July 2012. The defense has failed to provide an adequate basis for production of the remaining emails. The defense is invited to renew its request with more specificity and an adequate basis for its request.

4. Any other e-mails or documentation that the Government is aware of and has not previously provided to the Defense dealing with PFC Manning's confinement conditions while at Quantico.

**RESPONSE:** Absent what is stated above in response to paragraph 3, the e-mail in paragraph 8, and prosecution work product, the prosecution is not aware of any other e-mail or documentation dealing with the accused's confinement conditions while at Quantico.

5. The prosecution contacted, or attempted to contact, the below individuals for any e-mails or documentation relating to the accused or the accused's confinement conditions. The prosecution responds to the defense's request as follows:

a. LtGen George J. Flynn: LtGen Flynn is aware of any emails or documentation related to the accused or the accused's confinement conditions. LtGen Flynn is currently on retained records and the prosecution will notify the defense if any such material is found.

b. Col Christopher Miner: Col Miner is currently deployed to Afghanistan and is on R&R leave. The prosecution briefly spoke with Col Miner who stated he will review his files when he returns to Afghanistan. The prosecution will notify the defense if any such material is found.

c. Col Royal Mortenson: Col Mortenson does not have any email or documentation related to the accused or the accused's confinement conditions.

d. Col Carl R. Cottman Jr.: Col Cottman does not have any email or documentation related to the accused or the accused's confinement conditions. Outside what has already been produced or provided to the defense, the prosecution will not identify additional information.

● (13-14 August 2012) the prosecution searched various email servers for e-mails that have not previously produced to the defense. The first document (BAC: S-100570078-00000841) is a confirmed e-mail in which certain information previously produced to the defense may be the subject of litigation and public affairs pages were not produced. The second document (BAC: S-100570078-00000841) is a page purchased pursuant to a wordless telephone number purchase (13-14 August 2012).



signed by the COJ. Coffman related to the accused's pretrial confinement not later than 17 August 2012.

e. Col Daniel J. Choike. Col Choike does not have any emails or documentation related to the accused or the accused's confinement conditions, in addition to the what he provided LTC of Greer pursuant to the prosecution's preservation request.

f. Col Mark M. Kauzanchi. Col Kauzanchi does not have any emails or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, Col Kauzanchi provided all emails or documentation to LTC of Greer.

g. CDR Han Bar. CDR Bar does not have any emails or documentation related to the accused or the accused's confinement conditions. According to CDR Bar, any notes would have been annotated in the accused's medical records, which have already been produced to the defense.

h. CAPT Mary Neill. CAPT Neill does not have any emails or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, CAPT Neill provided all emails or documentation to LTC of Greer.

i. LTC Christopher M. Greer. LTC of Greer does not have any emails or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, LTC of Greer provided all emails or documentation to the prosecution.

j. LTCol Amy R. Ebitz. LTCol Ebitz is currently assigned on ONS and is currently on Temporary Duty without means of communication. The prosecution has been unable to correspond with LTCol Ebitz and will notify the defense if any such material is found.

k. CPT John Haberland. CPT Haberland was a member of the prosecution team until he was designated as the legal subject matter expert for external public affairs on 16 May 2012. Any emails prior to that time are work product, including his emails concerning Quantico. Since then, CPT Haberland's role has been limited solely to public relations, not the prosecution of the accused.

l. CWO5 Abel Galaviz. CWO5 Galaviz does not have documentation, including his own report, emails, status reports, and notification.

m. CWO4 James L. Averhart. CWO4 Averhart does not have any email or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, CWO4 Averhart provided all emails or documentation to LTC of Greer.

n. CWO2 Denise Barnes. CWO2 Barnes does not have any emails or documentation related to the accused or the accused's confinement conditions, in addition to the what she provided LTC of Greer pursuant to the prosecution's preservation request.

o MSgt Brian R. Papakie: MSgt Papakie does not have any emails or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, MSgt Papakie provided all emails or documentation to LTCol Greer.

p MSgt Craig M. Blenis: MSgt Blenis does not have any emails or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, MSgt Blenis provided all emails or documentation to LTCol Greer.

q GSgt William R. Fuller: GSgt Fuller does not have any emails or documentation related to the accused or the accused's confinement conditions. Pursuant to the prosecution's preservation request, GSgt Fuller provided all emails or documentation to LTCol Greer.

6. The prosecution understands its continuing obligation to produce material under § 660 and Rule for Courts-Martial (RCM) 914. See Giglio v. United States, 405 U.S. 413 (1972); see also RCM 914. Once the prosecution publishes its Article 15 witness list, it will immediately start the process of conducting Giglio and Jefferis searches.

J. C. NICHOLS, JYTF  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. Daniel Coombs, Civilian Defense Counsel, via electronic mail, on 14 August 2012.

J. BRUNER WILLY  
CPT, JA  
Assistant Trial Counsel

# ATTACHMENT D

## David Coombs

---

**From:** Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>  
**Sent:** Thursday, July 26, 2012 7:49 PM  
**To:** David Coombs  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR \MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** Article 13 Emails

David,

In preparation for the upcoming Article 13 motion, the prosecution began reviewing emails yesterday from members of the Quantico brig staff and the chain of command. The prosecution found some emails that are obviously material to the preparation of the defense for Article 13 purposes. In an effort to get these emails to you as soon as possible, we intend to produce them tomorrow and send them to you via email so that you have a copy immediately. We will also produce them according to our normal process. We estimate there are approximately 60 emails.

V/r  
Ashden

# ATTACHMENT E

## David Coombs

---

**From:** Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>  
**Sent:** Friday, July 27, 2012 8:22 AM  
**To:** Lind, Denise R COL USARMY (US)  
**Cc:** David Coombs; Hurley, Thomas F MAJ OSD OMC Defense; Tooman, Joshua J CPT USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S, CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** RE: Article 13 Emails

Ma'am,

Below is the government response to the below email from the defense.

1. On 8 December 2010, the defense requested "[a]ny and all documents or observation notes by employees of the Quantico confinement facility relating to PFC Bradley Manning." The United States produced all documentation from the Quantico Brig either as we received it or at the end of the accused's pretrial confinement at Quantico. In an effort to preserve all records involving the accused, the prosecution requested Quantico preserve all documentation and their emails. The purpose of this preservation request was to ensure the accused's right to a fair trial by preserving any emails for future litigation concerning the discoverability of the emails and/or for the prosecution to conduct a Giglio and Jencks (RCM 914) check of the emails. On Wednesday, the prosecution started reviewing the emails for potential impeachment evidence or Jencks material, and during that review found 84 emails which we deemed obviously material to the preparation of the defense for Article 13 purposes. Within 24 hours, the United States notified the defense and sent the emails last night.
2. The United States objects to the defense's characterization of the emails showing a conspiracy, rather the emails show the possible extent, if any, of USMC chain of command's involvement, in the accused's pretrial confinement.
3. This motions hearing is not scheduled until the end of August. Over the past few months, the defense has been preparing its over 100 page motion and the government has a reply due on 17 August 2012. Understanding Mr. Coombs will be out of the office from 27 July to 9 August, the United States still sees no reason why the defense will not have adequate time to prepare its Article 13 motion, and especially since this the majority of these emails appear to only bolster the defense's current argument, as proffered in the Article 13 witness list litigation. Additionally, the military defense counsel can assist Mr. Coombs with interviewing other potential witnesses, if the defense chooses to go down that path.

v/r  
MAJ Fein

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]  
Sent: Friday, July 27, 2012 12:54 AM  
To: Lind, Denise R COL USARMY (US)  
Cc: Hurley, Thomas F MAJ OSD OMC Defense; Tooman, Joshua J CPT USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S, CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
Subject: RE: Article 13 Emails  
Importance: High

Ma'am,

Please see the email below. MAJ Fein just notified the Defense of the existence of 60 emails that the Government determined were material to the

# ATTACHMENT F

## David Coombs

---

**From:** Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>  
**Sent:** Tuesday, August 14, 2012 5:30 PM  
**To:** David Coombs  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** RE: Discovery Response, 1 Aug 12

David,

We received a total of 1374 emails, and after reviewing them, produced 84, which leaves 1290 remaining.

v/r  
Ashden

-----Original Message-----

**From:** David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
**Sent:** Tuesday, August 14, 2012 5:15 PM  
**To:** Fein, Ashden MAJ USARMY MDW (US)  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** RE: Discovery Response, 1 Aug 12

Ashden,

Before I alert the Court to the need for a motion to compel, can you tell me how many other emails you have in addition to the 84 that you provided to the Defense?

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
[www.armycourt martialdefense.com](http://www.armycourt martialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*



## David Coombs

---

**From:** Overgaard, Angel M CPT USARMY (US) <angel.m.overgaard.mil@mail.mil>  
**Sent:** Sunday, July 29, 2012 2:21 PM  
**To:** David Coombs  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Fein, Ashden MAJ USARMY MDW (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR \MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); von Elten, Alexander S (Alec) CPT USARMY (US)  
**Subject:** RE: Quantico Emails (UNCLASSIFIED)

Classification: UNCLASSIFIED  
Caveats: NONE

David,

MAJ Fein used the phrase "obviously material to the defense" because that is what is required by the 22 June 2012 Court Order. That being said, the prosecution disclosed the emails that were "material to the preparation of the defense."

VR  
ANGEL M. OVERGAARD  
CPT, JA  
Trial Counsel, MDW

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
Sent: Friday, July 27, 2012 8:46 PM  
To: Overgaard, Angel M CPT USARMY (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Fein, Ashden MAJ USARMY MDW (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
Subject: Quantico Emails

Angel,

With regards to the Quantico emails, MAJ Fein used the phrase "obviously material to the defense." I wanted to make sure that the Government did not have any emails in its possession that were "material to the preparation of the defense" as opposed to "obviously material to the preparation of the defense."

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)

[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

Classification: UNCLASSIFIED

Caveats: NONE

## David Coombs

---

**From:** Morrow, JoDean (Joe) III CPT USARMY USAMDW (US) <jodean.morrow.mil@mail.mil>  
**Sent:** Tuesday, July 31, 2012 2:43 PM  
**To:** David Coombs; Overgaard, Angel M CPT USARMY (US); Overgaard, Angel M CPT USARMY (US)  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Fein, Ashden MAJ USARMY MDW (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCRMDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Fein, Ashden MAJ USARMY MDW (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCRMDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US)  
**Subject:** RE: Update (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

David,

Filing dates - Angel responded yesterday, but we've been experiencing some email difficulties. With respect to the speedy trial filings, we have no issues with your counter-offer. Motion due on 26 September; Response due on 16 October; Reply due on 22 October.

Emails - We disclosed all the emails from Quantico in our possession that are material to the preparation of the defense. We made a generalized request for Quantico to gather and preserve documents and information pertaining to PFC BM's confinement. They responded by providing documents and information pertaining to his confinement, and included some emails.

Meeting - We are already working on the meeting request.

CPT Joe Morrow  
Trial Counsel  
U.S. Army Military District of Washington  
Phone: 202-685-1975  
NIPR: [jodean.morrow.mil@mail.mil](mailto:jodean.morrow.mil@mail.mil)  
SIPR: [jodean.morrow@jfhqncr.northcom.smil.mil](mailto:jodean.morrow@jfhqncr.northcom.smil.mil)

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
Sent: Tuesday, July 31, 2012 11:56 AM  
To: Overgaard, Angel M CPT USARMY (US); Overgaard, Angel M CPT USARMY (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Fein, Ashden MAJ USARMY MDW (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCRMDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); von Elten, Alexander S (Alec) CPT USARMY (US); 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Fein, Ashden MAJ USARMY MDW (US); Whyte, J

Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCRMDW SJA'; Ford, Arthur D Jr CW2 USARMY (US);  
Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); von Elten, Alexander S (Alec) CPT USARMY (US)  
Subject: Update (UNCLASSIFIED)

Angel,

Can you please provide me with an update on the following:

- a) The proposed dates for the Speedy Trial motion; and
- b) The Government's access to other emails from the listed individuals (1) LTG George Flynn; 2) Col. Daniel Choike; 3) Col. Robert Oltman;
- 4) COL Carl Coffman; and 5) LtCol. Christopher Greer.

Finally, could you please arrange for PFC Manning to be brought to Fort Meade TDS at 1330 on 27 August 2012? Thank you.

Best,

David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)

[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com) <<http://www.armycourtartialdefense.com/>>

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

Classification: UNCLASSIFIED

Caveats: NONE

## David Coombs

---

**From:** Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>  
**Sent:** Tuesday, August 14, 2012 5:30 PM  
**To:** David Coombs  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** RE: Discovery Response, 1 Aug 12

David,

We received a total of 1374 emails, and after reviewing them, produced 84, which leaves 1290 remaining.

v/r  
Ashden

-----Original Message-----

**From:** David Coombs [<mailto:coombs@armycourtartialdefense.com>]  
**Sent:** Tuesday, August 14, 2012 5:15 PM  
**To:** Fein, Ashden MAJ USARMY MDW (US)  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** RE: Discovery Response, 1 Aug 12

Ashden,

Before I alert the Court to the need for a motion to compel, can you tell me how many other emails you have in addition to the 84 that you provided to the Defense?

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Response

to Defense Motion to  
Compel Discovery #3

23 August 2012

RELIEF SOUGHT

The United States respectfully requests the Court deny, in part, the Defense Motion to Compel Discovery #3 (Defense Motion) because the United States will produce all emails of witnesses of both parties and all emails required under *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), the Jencks Act, 18 U.S.C. § 3500, Rule for Courts-Martial (RCM) 701(a)(2), RCM 701(a)(6), and RCM 914.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the Defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. *See Manual for Courts-Martial (MCM), United States, RCM 905(c) (2012).*

FACTS

The United States stipulates to Defense Motion ¶¶ 4-6.

The United States stipulates to Defense Motion ¶ 7. The United States and Defense have proposed multiple filing dates, to include 15 June 2012, 27 July 2012, and 7 September 2012 for the Defense Motion to Dismiss for Unlawful Pretrial Punishment (Defense Article 13 Motion). *See* Appellate Exhibit I, Appellate Exhibit XX, Appellate Exhibit XLIV, Appellate Exhibit XLV, Appellate Exhibit CXIII

The United States stipulates to Defense Motion ¶ 8.

The United States stipulates to Defense Motion ¶ 9; however, the United States disputes the Defense description of the contents of the emails.

The United States stipulates that the Defense requested a continuance of the proceedings and that the Court granted the Defense's request on 1 August 2012.

On 8 December 2010, the Defense submitted a discovery request, requesting "[a]ny and all documents or observation notes by employees of the Quantico confinement facility relating to [the accused]." Enclosure 1 ¶ 2(m). In the same discovery request, the Defense requested "[a]ny report, e-mail or document discussing the need for the State Department to disconnect access to its files from the government's classified network." *Id.* ¶ 2(b) (emphasis added). The discovery

request also requested, “[a]ny e-mail, report, assessment, directive, or discussion by President Obama to the Department of Defense, Department of State or Department of Justice.” *Id.* ¶ 2(f) (emphasis added). The discovery request further requested, “any and all memorandums, e-mails, or other references by Congressmen, Senators, or government officials concerning the disposition of this case or the need to punish [the accused].” *Id.* ¶ 2(k) (emphasis added). The discovery request requested, “[a]ny and all documentation, e-mails, or reports given to the Summary Court-Martial Convening Authority, the General Court-Martial Convening Authority, or the Staff Judge Advocate concerning the disposition of [the accused’s] case or nature of the charges or possible charges against [the accused].” *Id.* ¶ 2(l) (emphasis added).

On 1 August 2012, the Defense filed a discovery request, requesting, “[a]ll documentation provided . . . in response to the Government’s [prudential search request],” and “any other e-mails or documentation that the Government is aware of . . . dealing with [the accused’s] confinement conditions while at Quantico.” See Enclosure 2 ¶ 6(c)-(d).

On 17 August, the Defense filed the Defense Motion, stating that “that the Defense believed [the accused’s] confinement conditions were unnecessarily onerous.” Defense Motion ¶ 17. The Defense Motion also stated that the accused “had repeatedly requested to be removed from [maximum custody] and [prevention of injury status].” *Id.* The Defense stated that the emails demonstrate “the extent of involvement by individuals outside of the Quantico Brig in the custody status and classification of [the accused].” Defense Motion ¶ 19.

The United States will produce to the Defense the emails of the parties’ witnesses and emails material to the preparation of the defense on or before 28 August 2012.

#### WITNESSES/EVIDENCE

The United States does not request any witnesses be produced for this response. The United States respectfully requests that the Court consider the listed enclosures and Appellate Exhibits.

#### LEGAL AUTHORITY AND ARGUMENT

RCM 701(a)(2) requires the United States to permit the Defense to inspect documents that are material to the preparation of the defense that are within the possession, custody, or control of military authorities in response to a defense request. RCM 701(a)(2). The United States does not have to “search for information material to the preparation of the defense without a specific discovery request.” Appellate Exhibit CXLVII at 5. Instead, a defense request “specifying what must be produced” triggers the rule. Appellate Exhibit CXLVII at 5; RCM 701(a) analysis, at A21-34 (2012). The Defense request must provide notice with specificity of the information it desires. See *United States v. Eshalomi*, 23 M.J. 12, 22 (C.M.A. 1986) (citing *United States v. Agurs*, 427 U.S. 97, 106 (1976)). A request for all information fails to provide the United States with adequate notice. See *Agurs*, 427 U.S. at 106 (deciding that an indefinite request for all exculpatory information “really gives the prosecutor no better notice than if no request is made”). Additionally, the United States must turn over information to the Defense that



is obviously material to the preparation of the defense. See Appellate Exhibit CXLVII at 5; RCM 701(a) analysis, at A21-34 (2012).

RCM 701(a)(2) is “grounded on the fundamental concept of relevance. *United States v. Graner*, 69 M.J. 104, 107 (C.A.A.F. 2010). Relevant emails that would assist the Defense in formulating a strategy are material to the preparation of the defense. See *United States v. Webb*, 66 M.J. 89, 92 (C.A.A.F. 2008) (citing *United States v. Roberts*, 59 M.J. 323, 325 (C.A.A.F. 2004)). Additionally, the Defense defines material to the preparation of the defense as “relevant and helpful.” Defense Motion ¶ 21 (“The Government must turn over all documents which are material to the preparation of the Defense – as in relevant and helpful.”).

#### I. THE DEFENSE DID NOT TRIGGER RCM 701(A)(2) UNTIL 1 AUGUST 2012

On 26 July 2012, the United States produced eighty-four emails that were obviously material to the preparation of the defense without a request from the Defense for emails from the Brig. The Defense first requested emails from the Brig on 1 August 2012. See Enclosure 2 ¶ 6(d). The Defense contends that its 8 December 2010 discovery request for “[a]ny and all documents or observation notes by employees of the Quantico confinement facility relating to [the accused]” included email. See Defense Motion ¶ 16; but see Enclosure 1 ¶ 2(m). However, the Defense only requested “documents or observation notes” from the Brig. The Defense itself distinguished between documents and emails by requesting emails in four other separate requests in the same document. See Enclosure 1 ¶ 2(b); Enclosure 1 ¶ 2(f); Enclosure 1 ¶ 2(k); Enclosure 1 ¶ 2(l). The Defense now avers that the United States should not have made the distinction the Defense itself made in the Defense discovery request—the request the Defense now cites in support of its theory that it requested email from the Brig on 8 December 2010. See Defense Motion ¶ 16. Because the Defense distinguished between documents and emails within its own request, its claim that it requested email before 1 August 2012 lacks merit. Accordingly, Defense first requested emails from the Brig on 1 August 2012.

#### II. THE DEFENSE DID NOT PROVIDE NOTICE OF MATERIALITY UNTIL 17 AUGUST 2012

The Defense request on 1 August 2012 provided the United States with no notice of materiality because the Defense simply requested “any other e-mails” without even a scant provision of relevance or materiality. However, the Defense provided a basis for determining materiality in the Defense Motion on 17 August 2012 by stating that “the extent of involvement by individuals outside of the Quantico Brig in the custody status and classification of [the accused],” the conditions of the accused’s confinement “were unnecessarily onerous,” and the accused “repeatedly requested to be removed from [maximum custody] and [prevention of injury status].”

**Based on the stated standards and in preparation for the Article 39(a) during 1 to 5 October 2012, the United States will produce all emails of witnesses of both parties and all emails required under *Brady v. Maryland*, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), the Jencks Act, 18 U.S.C. § 3500, RCM 701(a)(2), RCM 701(a)(6), and RCM 914.**

The emails the United States has not produced are related to: 1) public affairs, to include discussions of media articles and preparing responses to media inquiries, including responses to media reports by the New York Times and Frontline, 2) protesters at Marine Corps Base Quantico (MCBQ), to include discussions of upcoming protests, the number of protestors, and plans to respond to protests, 3) discussions of operational impact on the Pretrial Confinement Facility (the Brig) at MCBQ based on projected detainees, the Defense Base Realignment and Closure Commission (BRAC), providing behavioral health support to detainees, to include the accused, 4) funding of behavioral health professionals, to include discussions of the extent of each Service's financial obligations, 5) administrative coordination, to include ensuring detainees, including the accused, had constant coverage of behavior health, ensuring the accused had the proper uniform, discussing the accused's "chasers," 6) discussions of the definition of Brig regulations regarding visits and statements of changes the accused made to his visitation list, 7) editing drafts of proposed documents, to include responses to media inquiries, 8) discussion of visits of officials to the Brig unrelated to the accused, and 9) discussions of complying with the Health Insurance Portability and Accountability Act (HIPAA).

The emails that were not produced are not helpful to the Defense's preparation because they pertain to matters unrelated to the conditions of the accused's confinement or matters not related to the accused's custody and classification. The Defense argues that the number of emails indicates "the involvement by individuals outside of the Quantico Brig," but the number of emails only indicates the breadth of issues to which the Brig responded during the accused's confinement for over eight months. The emails not produced are not relevant because they do not describe the conditions of the accused's confinement, nor do the emails pertain to decisions regarding the accused's classification or status. Moreover, the emails do not yield any insight into the conditions of the accused's confinement nor the accused's classification or status. Therefore, the emails not produced are not material to the preparation of the defense. The defense alleges that orders were given to keep the accused in a certain status and custody but there are no such orders. Seeing emails discussing responses to media inquiries or HIPAA compliance grants no insight to the Defense and therefore is not material to its preparation.

### CONCLUSION

Based on the above, the United States respectfully requests the Court deny, in part, the Defense Motion.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

#### Enclosures

1. Defense Discovery Request dated 8 December 2010
2. Defense Discovery Request dated 1 August 2012
3. Fein Email, "Government Notice to Court" dated 23 August 2012

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail, on 23 August 2012.

A handwritten signature in black ink, consisting of a stylized capital 'A' followed by a vertical line and a small loop at the top.

ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Response

to Defense Motion to  
Compel Discovery

Enclosure 1

23 August 2012

UNITED STATES )

v. )

**MANNING, Bradley E., PFC** )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE DISCOVERY  
REQUEST**

DATE D: 8 December 2010

1. In accordance with the Rules for Courts-Martial and the Military Rules of Evidence, Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, request for supplemental discovery is hereby made for the charged offenses in the case of United States v. Bradley E. Manning.

2. The defense requests that the government respond to each item listed in its 29 October and 15 November 2010 discovery requests and the following additional discovery:

- a) The names and contact information for all government investigators who have participated or who are presently participating in the investigation of the case, previously requested on 29 October and 15 November 2010. Specifically, contact information for SA Hyung Kim from the Department of Defense and SA Richard Bowen from the Army Computer Crimes Unit and an inventory of the items seized from the home of Mr. Paul Francia at 601 Hazelwood Terrace, Rochester, New York 14609.
- b) All forensic results and investigative reports by the Department of State regarding the information obtained by Wikileaks as referenced by Assistant Secretary of State for Public Affairs P.J. Crowley. Additionally, any specific damage assessment by the Department of State regarding the disclosures of the diplomatic cables by Wikileaks. Any assessment, report, e-mail, or document by Secretary of State Hillary Rodham Clinton regarding the disclosures of diplomatic cables by Wikileaks. Any report, e-mail, or document discussing the need for the State Department to disconnect access to its files from the government's classified network.
- c) All forensic results and investigative reports by the Department of Defense regarding the information obtained by Wikileaks and the results of any joint investigation with the Federal Bureau of Investigation (FBI) as referenced by Secretary of Defense Robert M. Gates. Additionally, any specific damage assessment by the Department of Defense regarding the disclosure of classified documents and videos, the subject of this case, by Wikileaks.

- d) Any and all documentation related to the Department of Justice investigation into the alleged leaks by WikiLeaks as referenced by Attorney General of the United States Eric H. Holder.
- e) Any and all documentation related to President Barack H. Obama's order for an investigation and a government wide-review of how agencies safeguard sensitive information. Additionally, any and all documents related to the steps the administration is considering regarding these leaks and the nature of the criminal investigation underway into how the documents were made public as referenced by Robert Gibbs, the White House spokesman.
- f) Any assessment given, or discussions concerning, the Wikileaks disclosures by any member of the government to President Obama. Any e-mail, report, assessment, directive, or discussion by President Obama to the Department of Defense, Department of State or Department of Justice.
- g) Any and all documents relating to the Government Task Force created to review the various WikiLeaks releases for potentially damaging information prior to the actual releases. This Task Force apparently had over 120 members reviewing the documents that were either released or pending release to determine the possible harm to national security.
- h) The results of any investigation or review by Mr. Russell Travers who has been appointed by President Obama to head an interagency committee assigned to assess the damage caused WikiLeaks exposures and to organize efforts to tighten security measures in government agencies.
- i) Any and all documentation related to the Pentagon's review on the policy and technological shortfalls that led to the WikiLeaks disclosures as referenced by Pentagon spokesman Bryan Whitman.
- j) Any and all documentation related to the Central Intelligence Agency (CIA) investigation of Wikileaks announced by CIA Director Leon Panetta and any internal or external memorandums addressing the investigation of Wikileaks, PFC Bradley Manning or the nature of the Office of Security's investigation into these matters.
- k) Any and all documentation relating to the government's position of taking a hard line on unauthorized leaks of information, as demonstrated by the prosecutions of a former National Security Agency official, a Federal Bureau of Investigation linguist, and a State Department contractor and referenced by CIA Director Leon Panetta. Additionally, any and all memorandums, e-mails, or other references by Congressmen, Senators, or government officials concerning the disposition of this case or the need to punish PFC Bradley Manning.

l) Any and all documentation, e-mails, or reports given to the Summary Court-Martial Convening Authority, the General Court-Martial Convening Authority, or the Staff Judge Advocate concerning the disposition of PFC Bradley Manning's case or the nature of the charges or possible charges against PFC Manning. Specifically, any attempt to influence the independent discretion of anyone involved in the military justice process.

m) Any and all documents or observation notes by employees of the Quantico confinement facility relating to PFC Bradley Manning.

n) The results of the 15-6 investigation into the government's improper release of classified information to the defense. Whether the 15-6 investigating officer looked into the following additional potential spillage:

i. The disc allegedly found in PFC Manning's Room indicated the contents were SECRET. A photo of the disk can be found at 000293. Was the title on the disk classified or not?

ii. The photos of the T-SCIF show a map in the background that was partially exposed (000301 and 000302).

iii. The snapshots of the computer screens in the T-SCIF were exposed. Was there classified information being viewed on the screen? (000305 and 000306).


iv. The snapshots of the computers had documentation on the table appear to show classified information. (000333, 000334, and 000335).

v. Was the investigating officer made aware of the government disclosure of the original five discs to the military defense counsel?

3. The defense requests that the government inform the defense counsel if it does not intend to comply with any specific provision of this request.

4. It is understood that this is a continuing request.

5. A copy of this request was served on Trial Counsel by e-mail on 8 December 2010.

  
DAVID EDWARD COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Response  
to Defense Motion to  
Compel Discovery

Enclosure 2

23 August 2012



UNITED STATES

v.

**MANNING, Bradley E., PFC**

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE DISCOVERY  
REQUEST**

DATED: 1 August 2012

1. In accordance with the Rules for Courts-Martial 701(a)(2), 701(a)(6) and the Military Rules of Evidence, Manual for Courts-Martial, United States, 2008, Article 46, Uniform Code of Military Justice, and other applicable law, request for discovery is hereby made for the charged offenses in the case of United States v. Bradley E. Manning.

2. PFC Manning was held at Marine Corps Base Quantico from 29 July 2010 to 20 April 2011. During this time, he was held in Maximum Custody (MAX) and under Prevention of Injury (POI) watch.

3. On 8 December 2010, the Defense made a discovery request for all documentation from Quantico pertaining to PFC Manning. The Government provided extensive documentation related to PFC Manning's confinement at Quantico in October of 2011. The Defense believed that this was the full extent of the information the Government had from Quantico.

4. On 26 August 2012, the Government produced 84 emails from various individuals. The Government indicated that these emails were "obviously" material to the preparation of the defense for the Article 13 purposes. MAJ Fein indicated that the Government received these emails from Quantico approximately 6 months ago. However, the Government did not begin reviewing the emails until 25 July 2012.

5. On 31 August 2012, CPT Joe Morrow, by e-mail, informed the Defense that the Government had "made a generalized request for Quantico to gather and preserve documents and information pertaining to PFC Manning's confinement." CPT Morrow stated that "they responded by providing documents and information pertaining to his confinement, and included some emails."

6. The Defense requests that the Government provide the following discovery:

- a) The memorandum/e-mail/document from the Government to Quantico requesting that they preservation and produce documents and information pertaining to PFC Manning's confinement;
- b) The names of the individuals who the Government sent the Quantico preservation request to and the date which the Government made its request;

Defense Discovery Request – PFC Bradley E. Manning

- c) All documentation provided by these individuals in response to the Government's request, the date this information was provided, and the individuals who provided the requested information; and
  - d) Any other e-mails or documentation that the Government is aware of and has not previously provided to the Defense dealing with PFC Manning's confinement conditions while at Quantico.
7. The Defense also requests any e-mails or documentation relating to PFC Manning or PFC Manning's confinement conditions from or to the following specifically listed individuals:
- a) LtGen. George J. Flynn, george.j.flynn@usmc.mil, Commanding General, 3300 Russell Road Building: 3300 Floor: 2 Room, Quarters 1 / Command Suite, Quantico, VA 22134. (703) 784-2416;
  - b) Col. Christopher Miner, christopher.miner@usmc.mil, Staff Judge Advocate, 3300 Russell Road Building 3300 Floor 2, Room 227, Quantico, VA 22134 (703) 432-8168;
  - c) Col. Royal Mortenson, royal.mortenson@usmc.mil, Chief of Staff, 3300 Russell Road Building: 3300 Floor: 2 Room: 224, Quantico, VA 22134. (703) 784-2665;
  - d) COL Carl R. Coffman Jr., carl.coffman@us.army.mil, 205B Lee Avenue, Joint Base Myer-Henderson Hall, Virginia 22211. (912) 257-8747;
  - e) Col. Daniel J. Choike, daniel.choike@usmc.mil, Base Commander, 3250 Catlin Ave., Building 3250, Floor 2, RoomCube Cmd Suite, Quantico, VA 22134. (703) 784-5900;
  - f) Col. Mark M. Kauzlarich, mark.kauzlarich@usmc.mil, Chief of Staff, 3250 Catlin Ave., Building 3250, Floor B, Room 28, Quantico, VA 22134 (703) 784-5911;
  - g) CDR Han Bui, han.bui@med.navy.mil, Building 1A Floor 2, Room 9, Norfolk, VA 23511 (757) 953-0515;
  - h) Capt. Mary Neill, mary.neill@med.navy.mil, (703) 784-1500;
  - i) LtCol. Christopher M. Greer, christopher.m.greer@usmc.mil, Staff Judge Advocate, Building: 1019, Floor: 1, Room: SJA, Quantico, VA 22134 (703) 432-1578;
  - j) LtCol. Amy R. Ebitz, amy.ebitz@usmc.mil, Executive Officer, 2043 Baranett Ave, Quantico, VA 22134 (703) 784-2385.
  - k) CPT John Haberland, john.haberland@us.army.mil, Regimental Judge Advocate, 201 Jackson Ave, Fort Myer, VA 22003. (703) 696-3150;
  - l) CW05 Abel Galaviz, abel.galaviz@usmc.mil, Building Pentagon, Floor 4, Room/Cube 4A324, Washington D.C., 20380-1775. (703) 614-1480;

Defense Discovery Request – PFC Bradley E. Manning

- m) CWO4 James T. Averhart, james.averhart@usmc.mil, S-3 Officer, 2043 Baranett Ave, Quantico, VA 22134 (703) 784-4423;
- n) CWO2 Denise Barnes, denise.barnes@usmc.mil, Brig Executive Officer, Camp Hansen Bldg: Floor 1, Room 107, PFO, AP (315) 623-4698;
- o) MSgt Brian R. Papakie, brian.papakie@usmc.mil, Brig Supervisor, 3247 Elrod Ave Building: 3247 Floor 1, Room 110, Quantico, VA 22134 (703) 784-2718;
- p) GySgt Craig M. Blenis, craig.blenis@usmc.mil, Sergeant Instructor, 2189 Elrod Ave Building 5001, Floor 1, Room 1, Quantico, VA 22134 (703) 432-6075; and
- q) GySgt William R. Fuller, william.fuller@usmc.mil, PSC 561, Building 608, Floor, 1 Room/Cube 211, FPO, AP. (315) 253-3467.

8. The Defense requests that the Government provide notice in writing as soon as possible if it does not intend to comply with any specific provision of this request. The Defense will need timely notice of the Government's intent to not comply in order to immediately file a motion to compel discovery. Timely notice by the Government will avoid the need for an additional delay for the Article 13 motion.

9. It is understood that this is a continuing request.

10. A copy of this request was served on Trial Counsel by e-mail on 1 August 2012.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Response

to Defense Motion to  
Compel Discovery

Enclosure 3

23 August 2012

**From:** Fein, Ashden MAJ USARMY MDW (US)  
**To:** Lind, Denise R COL USARMY (US)  
**Cc:** David Coombs; "Hurley, Thomas F MAJ OSD OMC Defense"; Tooman, Joshua J CPT USARMY (US); Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US); Williams, Patricia A CIV (US); Jefferson, Dashaun MSG USARMY (US); Moore, Katrina R SFC USARMY (US)  
**Subject:** Government Notice to Court  
**Date:** Thursday, August 23, 2012 11:25:41 AM  
**Attachments:** Jencks.msg  
Classified Information Access.msg  
**Importance:** High

---

Ma'am,

Good morning. The purpose of this email is to provide the Court notice and an update on two issues to prevent any surprises or confusion during the upcoming hearing and to capture these two issues for the record.

1. Jencks Disclosure. On 26 July 2012, the Court directed the United States to notify the defense by 3 August what type of statements the government intends to disclose to the defense IAW RCM 914 (see email, 26 July 2012, 5:40pm). The Court directed the defense to file a motion by 17 August if it took issue with the government's plan. On 3 August, the government provided the attached notice to the defense and an email conversation ensued. The defense did not object to the government interpretation of Jencks or its plan moving forward, nor did they file a motion on 17 August 2012. Therefore, this issue should be resolved. As of today, the United States will move forward with its plan to begin disclosing statements encompassed by RCM 914, starting with designated witnesses for the Article 13 motion.

2. Defense Motion to Amend the Protective Order. On 17 August 2012, the defense requested leave of the Court to use a computer that was not authorized under the Court's protective order and SIPRNET for its filing. The Court instructed both parties that this issue would be addressed at the next Article 39(a) session and that both parties should confer to determine if there is a mutually agreeable solution (see email, 17 August 2012, 4:23pm). The defense had not requested from the government to use that computer or SIPRNET prior to its filing on Friday. Since Monday of this week, the prosecution has attempted to coordinate with the defense and appropriate entities within the US Army to determine capabilities and authorities. At this point, without the information we have requested from the defense (enclosed on email and listed below), the prosecution will not be able to formulate a position on behalf of the government, to include supporting the defense's request, supporting it in part, or objecting, if at all. Without walking into the defense's office and examining their systems ourselves, the prosecution is not in a position to understand their capabilities. Therefore, without this information and a reasonable amount of time to work through the capabilities and approvals, the United States will be objecting to the Court's consideration of this requested amendment at next week's hearing and requesting a continuance to properly staff this request. Ultimately, we think the protective order issue is an issue which the parties could mutually resolve without the Court's involvement, but we need more info from defense to move forward.

v/r  
MAJ Fein

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]  
Sent: Wednesday, August 22, 2012 7:03 PM  
To: Fein, Ashden MAJ USARMY MDW (US); "Hurley, Thomas F MAJ OSD OMC Defense"; Tooman, Joshua J CPT USARMY (US)  
Cc: Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US)  
Subject: RE: Outstanding Emails

Ashden,

1. Please refer to the Court's email on 26 July 2012;
2. This issue is currently under advisement with the Court.

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
coombs@armycourt martialdefense.com  
www.armycourt martialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Fein, Ashden MAJ USARMY MDW (US)  
Sent: Wednesday, August 22, 2012 6:52 PM  
To: David Coombs; 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US)  
Cc: Morrow, JoDean (Joe) III CPT USARMY USAMDW (US); Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); von Elten, Alexander S (Alec) CPT USARMY (US); Ford, Arthur D Jr CW2 USARMY (US)  
Subject: Outstanding Emails  
Importance: High

David, MAJ Hurley, and CPT Tooman,

The United States sent the defense two separate emails yesterday which are attached. We have not heard back from any defense counsel as of tonight.

1. Could you please respond to the defense's position on Jencks, so that we may notify the Court, and properly respond to the defense motion to compel discovery 3, and start implementing our Jencks plan before the end of the week?
2. Could you please respond to the questions about access to classified information so that we may coordinate with HQDA and other organizations about the requirements, and determine the capabilities and proper authorities? We are trying to process this request as fast as possible so we can provide the defense and Court an update next week.

Thank you!

v/r  
Ashden

UNITED STATES OF AMERICA )

v. )

Defense Motion  
to Amend Protective Order

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, US. Army) )

Army Garrison, Joint Base Myer-Henderson Hall)

Fort Myer, Virginia 22211 )

17 August 2012

#### RELIEF SOUGHT

The Defense in the above-captioned case respectfully requests that this Court amend its 16 March 2012 Protective Order for Classified Information. Specifically, the undersigned defense counsel requests that (1) his office be identified as an approved location to store SECRET information relevant to this case, (2) his office be identified as an approved location to work on (including discuss) SECRET information relevant to this case, (3) the neighboring appropriate facility be identified as a location to review and store information classified at a higher-than-SECRET level, and (4) the individual and collective equipment in his current office be authorized to be used in furtherance of his representation of PFC Manning.

#### BURDEN OF PERSUASION AND BURDEN OF PROOF

The defense bears the burden of persuasion as the moving party. The burden of proof is by a preponderance of the evidence. RCM 905(c).

#### FACTS

This case involves thousands of pages of classified information.

The undersigned defense counsel was detailed to this case in May 2012. He made his first appearance before this Court in June. Then, he worked in a traditional office environment on Fort Belvoir with limited access to classified telecommunications or office equipment.

On 3 July, the undersigned, pursuant to a personnel action commenced in February, started work at his new office at the Office of Chief Defense Counsel for the Military Commissions. The undersigned currently works in an office in Arlington, Virginia. The undersigned is told that, because of the security posture in and around the building, he can openly store classified information in his actual office. The undersigned has the following equipment at his desk: an unclassified phone, an unclassified laptop computer with a NIPRNET connection, and a SECRET desktop computer with a SIPRNET connection. (The SIPRNET provides the capability of a "smil" email address through which SECRET emails can be sent with SECRET documents attached.) The undersigned can, with some coordination, also make classified copies, scan classified documents, hold meetings in a higher-than-SECRET facility, store documents in a higher-than-SECRET facility, and make classified phone calls.

#### WITNESSES/EVIDENCE

None.

## LEGAL AUTHORITY

Protective Order for Classified Information, 16 March 2012

## ARGUMENT

The Defense requests this Court re-examine paragraphs "l" and "m" of its 16 March Protective Order to grant the relief requested. Here are the specific changes believed appropriate:

- a. The "Area of Review" paragraph should be changed to include the undersigned's current office as well as the neighboring higher-than-SECRET facility. A change to this paragraph would require modification of subparagraphs l(1), l(2), and l(5).
- b. The restriction on copying classified documents (subparagraph l(3)) should be changed to allow the undersigned to print or copy classified discovery provided to him by the Government.
- c. The admonishment to only use the three government computers for classified filing should be changed to allow the undersigned to use his classified government desktop computer for purposes described in subparagraph l(4) as well as the three classified laptop computers already provided to the Defense.

There is disagreement between the parties as to the meaning of the Protective Order. The Defense would request that this Court explicitly authorize the undersigned to do the following.

- a. Use his SIPRNET computer and connection to classified networks in furtherance of his lawful preparation for this trial with no supervision.
- b. Communicate with the Government as well as the Court (through the Court Security Officer) about any procedural or substantive matter that should be discussed over a classified system. This communication would include, but not be limited to, a request for information as to how to access discovery provided to the Defense by the Government as well as filing classified documents with the Court Security Officer and providing a copy of those documents to the Government.

## CONCLUSION

The Defense respectfully requests that this Court amend its 16 March 2012 Protective Order for Classified Information. Specifically, the undersigned defense counsel requests that (1) his office be identified as an approved location to store SECRET information relevant to this case, (2) his office be identified as an approved location to work on (including discuss) SECRET information relevant to this case, (3) the neighboring appropriate facility be identified as a location to review and store information classified at a higher-than-SECRET level, and (4) the individual and collective equipment in his current office be authorized to be used in furtherance of his representation of PFC Manning.

*Thomas F. Hurley*  
THOMAS F. HURLEY  
MAJ, JA  
Defense Counsel



[REDACTED]

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Motion

for Preliminary Determination of  
Admissibility of Evidence  
(Computer-Generated Records)

3 August 2012

(U) RELIEF SOUGHT

(U//FOUO) The prosecution in the above case respectfully requests that this Court admit into evidence the following account information and logs in advance of trial: Open Source Center (OSC) log files for the accounts bmanning and bradass87; OSC user information screenshots for the accounts bmanning and bradass87; Intelink logs showing activity for IP addresses 22.225.41.22 and 22.225.41.40; and the Intelink Passport account information for the account bradley.e.manning. The prosecution seeks said relief to provide improved predictability and efficiency to the proceedings.

(U) This motion also serves as notice to the defense that the government intends on offering these documents as evidence under Military Rule of Evidence (MRE) 902(11).

(U) BURDEN OF PERSUASION AND BURDEN OF PROOF

(U) The burden of proof on any factual issue, the resolution of which is necessary to decide a motion, shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue, the resolution of which is necessary to decide a motion, shall be on the moving party RCM 905(c)(2). The United States has the burden of persuasion as the moving party.

(U) FACTS

(U) U.S. Army IP address 22.225.41.22 (hereinafter .22) was the Accused's primary SIPRNET computer at his work station in the Sensitive Compartmented Information Facility (SCIF) at FOB Hammer, Iraq. See Enclosure 1. U.S. Army IP address 22.225.41.40 (hereinafter .40) was the Accused's secondary SIPRNET computer at his work station in the SCIF at FOB Hammer. See Enclosure 2.

(U//FOUO) The Accused had an Intelink passport account. Intelink passport accounts have user names and passwords, and the Accused was assigned the user name bradley.e.manning See Enclosures 4 and 9. The email address bradley.manning@us.army.smil.mil was assigned to the account, and the account was last used on 27 April 2010. See Enclosure 4

[REDACTED]

1

[REDACTED]

APPELLATE EXHIBIT 211  
PAGE REFERENCED: 211  
PAGE    OF    PAGES

[REDACTED]

(U) The Intelink passport account profile contains the identifying information of the user as well as personalized information in the form of questions and answers. See Enclosure 9.

[REDACTED]

(U) Intelink is the central SIPRNET search engine, analogous to www.google.com. While an Intelink search is the equivalent of an Internet Google search, Intelink searches websites only available via the SIPRNET. Searches using Intelink are typically logged. See Enclosure 3.

(U//FOUO) The Intelink log files revealed communications between the Accused's IP addresses in Iraq (.22 and .40) and the Intelink servers. See Enclosure 3. The Intelink logs captured search terms that were searched on SIPRNET, as well as files that were downloaded. See Enclosures 3 and 8.

[REDACTED]

(U) The significance of the searches for "julian+assange" is that Julian Assange was the co-founder and head spokesman of Wikileaks.org. The significance of the searches for "iceland" is that on 18 February 2010, Wikileaks.org posted a classified Department of State cable from the U.S. Embassy in Reykjavik, Iceland. See Enclosure 3. The significance of the searches relating to cracking passwords was that in recovered chat logs on the Accused's personal computer, the Accused discussed using the same password cracking tools. The significance of the searches relating to TOR is that TOR is a distributed network of virtual tunnels that allows users to hide their actions while on the Internet and was used on the Accused's personal computer. See Enclosure 3. The significance of the "collateral murder," "reuters," or "12 Jul 07" searches is that Collateral Murder was the name given to a movie created by WikiLeaks.org and released on 5 April 2010 concerning an Apache helicopter air strike involving the death of a Reuters reporter in 2007. See Enclosure 3.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) The OSC user account bradass87 was tied to the SIPRNET email address bradley.manning@us.army.smil.mil and was last used on 17 April 2010. See Enclosures 4 and 6. The Accused's AOL Instant Messenger username was bradass87. See Enclosure 4. The OSC account bmaning was tied to the SIPR email address bradley.manning@2bct10mtn and was last used on 6 November 2009. See Enclosures 4 and 5.

[REDACTED]

(U//FOUO) Between 17 March 2010 and 22 March 2010, the Accused's user account on his .22 computer accessed the files redcell\_afghanistan.pdf and redcell\_us\_exporter\_terrorism.pdf, both located in the folder C:\Documents and Settings\bradley.manning\My Documents\blah\.

See Enclosure 4.

(U//FOUO) A user of the Accused's personal computer accessed a CD/DVD named 100322\_1255 which contained the file blah.zip. The Accused's primary SIPRNET computer was configured to burn CD/DVDs and label them in a manner of YYMMDD\_HHMM. See Enclosure 4.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) WITNESSES/EVIDENCE

(U) The prosecution requests the Court consider the following: Charge Sheet and Listed Enclosures.

(U) LEGAL AUTHORITY AND ARGUMENT

(U) The trial judge has discretion as to the manner in which she makes preliminary determinations concerning the admissibility of evidence. MRE 104; see U.S. v. Blanchard, 48 M.J. 306 (C.A.A.F. 1998). This judicial discretion includes "preadmitting" evidence provided it is relevant and no other rule prohibits its admission. See, e.g., U.S. v. Bradford, 68 M.J. 371 (C.A.A.F. 2010). Where, as here, there is no question as to the admissibility of the evidence, the enclosed computer-generated records should be preadmitted to provide predictability to both parties and to dispose of what amounts to administrative matters outside the presence of the panel (assuming there is a panel).

I. (U) THE RECORDS ARE RELEVANT.

(U) Evidence that has a tendency to make a fact of consequence more or less probable than it would be without the evidence is relevant. MRE 401. All relevant evidence is generally admissible. MRE 402.

A. (U) OSC Logs and User Account

(U) The OSC user account information reveals that bradass87 and bmanning were the Accused's user accounts, and the OSC logs show the Accused's activity on OSC.

[REDACTED]

B. (U) Intelink Logs and Intelink Passport Account

(U//FOUO) The Intelink Passport Account information is relevant to all the charged misconduct because it reveals that the bradley e. manning account was set up and utilized by the Accused. See Enclosure 9.

[REDACTED]

[REDACTED]

(U) The Intelink logs are relevant to proving the charged misconduct in all the charges. They establish searches by the Accused for terms relating to all the charged misconduct. See Enclosure 8.

II. (U) THE RECORDS ARE NOT EXCLUDABLE AS HEARSAY BECAUSE THEY ARE COMPUTER GENERATED ACTIVITY

(U) Hearsay is an out of court statement, written or oral, offered for the truth of the matter asserted. MRE 801(c). A statement is an oral or written assertion or the nonverbal conduct of a person, if it is intended by the person as an assertion. MRE 801(a). A declarant is a person who makes a statement. MRE 801(b). A person must make a statement for it to be hearsay; a machine, therefore, cannot make a statement. See also Appellate Exhibit CCXVI ("machine generated data and printouts are not statements and, thus, they are not hearsay").

(U) United States v. Blazier, 69 M.J. 218 (C.A.A.F. 2010) is instructive on distinguishing between hearsay and computer generated records. In reviewing what portions of a drug testing report were admissible in a wrongful use case, the Court determined that testimonial hearsay included a signed, certified cover memorandum prepared at the request of the government for use at trial in which a person summarized the lab analyses. Id. at 221 fn.1. A person had written out what tests were conducted, what substances were detected, and the levels of each substance detected. Id. at 226. The cover memorandum was a written summary of the testimony that would be offered on the drug testing and its results.

(U) The Blazier Court then distinguished the testimonial hearsay in the cover memorandum from machine generated records, such as raw data and calibration charts, stating: "it is well-settled that under both the Confrontation Clause and the rules of evidence, machine-generated data and printouts are not statements and thus not hearsay - machines are not declarants—and such data is therefore not 'testimonial.'" Id. at 224 (citing United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008), United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Washington, 498 F.3d 225, 230-31 (4th Cir. 2007), United States v. Hamilton, 413 F.3d 1138, 1142-43 (10th Cir. 2005); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003)). According to the Court, "[m]achine-generated data and printouts such as those in this case are distinguishable from human statements, as they 'involve so little intervention by humans in their generation as to leave no doubt they are wholly machine generated for all practical purposes.'" Blazier, 69 M.J. at 224 (quoting Lamons, 532 F.3d at 1283 n.23).

(U//FOUO) Since the OSC logs and user account information screenshots, as well as the Intelink logs and Passport Account information are computer-generated, and thus not made by people, they cannot be hearsay.

[REDACTED]

[REDACTED]

III. (U) THE RECORDS ARE AUTHENTIC.

(U) In addition to being relevant, evidence must also be authentic to be admissible. See MRE 901(a). "[A]dmissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." MRE 901(a). Some evidence, however, is self-authenticating and does not require "[e]xtrinsic evidence of authenticity as a condition precedent to admissibility." MRE 902. "Certified domestic records of regularly conducted activity" fall under this exception. MRE 902(11)

(U) Pursuant to MRE 902(11), extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to certified domestic records of a regularly conducted activity when:

[t]he original or a duplicate of a document or record of regularly conducted activity that would be admissible under Mil. R. Evid. 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority certifying that the record (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) was kept in the course of the regularly conducted activity; and (C) was made by the regularly conducted activity as a regular practice.

MRE 902(11).

(U) "Records of regularly conducted activity" is defined in MRE 803(6) as the following:

[a] memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Mil. R. Evid. 902(11) or any other statute permitting certification in a criminal proceeding in a court of the United States, unless the source of the information or the method or circumstances or preparation lack trustworthiness.

MRE 803(6).

[REDACTED]

[REDACTED]

(U) The following attestations were made for the enclosed computer-generated files

(U//FOUO) On 22 June 2012, Mr. Stephen Buchanan, Information System Security Manager, National Security Agency, Fort Meade, MD, attested to the authenticity of the Intelink logs for both the computer used by the Accused in Iraq and the Intelink Passport account information for the Accused. Specifically, Mr. Buchanan attested to the following: the listed logs for IP address 22.225.41.22, with date ranges of 9 November 2009 to 30 December 2009, 23 January 2010 to 11 February 2010, and 2 March 2010 to 12 May 2010; the listed logs for IP address 22.225.41.40, with date ranges of 9 November 2009 to 31 December 2009, 1 January 2010 to 28 February 2010, and 1 March 2010 to 21 May 2010; and the Intelink Passport account information for bradley.e.manning, contained in the file manning.Idif. See Enclosure 6

(U//FOUO) On 29 June 2012, Mr. Maxwell Allen, Database Administrator, Central Intelligence Agency, Washington, DC, attested to the authenticity of the OSC log files and user information files, specifically for those OSC accounts pertaining to the users bradass87 and bmanning. See Enclosure 7.

(U) Since the attestations accompanying all records were made in accordance with MRE 902(1), all the records are properly authenticated.

IV. (U) THE RECORDS ARE IN A FORM THAT IS BEING OFFERED AS AN ORIGINAL OR DUPLICATE UNDER THE ORIGINAL WRITING RULE, OR THERE IS ADMISSIBLE SECONDARY EVIDENCE TO PROVE THE CONTENTS OF THE RECORDS IAW MRE 1001-1008

(U) "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original, or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." MRE 1003. A duplicate is defined as "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic rerecording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original." MRE 1001(4). "The contents of an official record . . . including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct or attested to in accordance with Mil. R. Evid. 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given." MRE 1005.

(U) In the certifications for all of the enclosed records, the records custodian specifically states that the records are true and accurate or complete copies of the originals. There is no evidence that any of the original documentation may not be authentic, nor is there any circumstance present which would make the admission of a duplicate in lieu of the original unfair. The enclosures include official records, and all of them are business records. The duplicates, therefore, are admissible to the same extent as the originals

[REDACTED]

[REDACTED]

V. (U) THE PROBATIVE VALUE OF THE RECORDS IS NOT SUBSTANTIALLY  
OUTWEIGHED BY UNFAIR PREJUDICE.

(U) Courts may exclude relevant evidence if its probative value is substantially outweighed by the danger of unfair prejudice, confusion, or waste of time. MRE 403. Prejudice alone is not sufficient to warrant exclusion. Virtually all evidence is prejudicial to one party or another. To justify exclusion the prejudice must be unfair. United States v. Candelaria-Silva, 162 F.3d 698, 705 (1st Cir. 1998).

(U) In the instant case, the log records and user account information are extremely probative in that they track what was occurring on the computers used by the Accused and on the user profiles created by the Accused. The evidence is prejudicial to the Accused in that it builds the case against him; however, it is not unfairly prejudicial. All of the logs are relevant to the Accused and the charged offenses and are a direct result of the Accused's actions. The logs establish a timeline to make the events clear to the factfinder.

CONCLUSION

(U) Based upon the requirements for admissibility of evidence in accordance with MRE 104, MRE 401, MRE 402, MRE 403, MRE 801, MRE 803(6), and MRE 902(11), the Government respectfully moves this Court, pursuant to RCM 906(13) to pre-admit the OSC logs and user information and the Intelink logs and user information in Enclosures 5-9 because they are relevant to the charges at issue and computer-generated information. They will provide improved predictability and efficiency to the proceedings.

  
ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

(U) I certify that I served or caused to be served a true copy of the above on Defense Security Experts, via electronic mail, on 3 August 2012.

  
ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

(U) 9 Enclosures

[REDACTED]



- [REDACTED]
1. (U) Forensic Report MANNING SIPR 22.225.41.22 22 Sep 11 (attached to AE CLXXVIII as Enclosure 1)
  2. (U) Forensic Report MANNING SIPR 22.225.41.40 22 Sep 11 (attached to AE CLXXVIII as Enclosure 2)
  3. (U) Forensic Report Intelink Logs-22 Sep 11
- [REDACTED]

5. (U) OSC User Information Files (bmannng) with attestation
6. (U) OSC User Information Files (bradass87) with attestation
7. (U) OSC Logs (bmannng & bradass87) with attestation
8. (U) Intelink .22 & .40 Logs with attestation
9. (U) Intelink Passport Account Information with attestation

Appellate Exhibit 246,  
Enclosure 1

has been entered into  
the record as

Appellate Exhibit 178,  
Enclosure 1

Appellate Exhibit 246,  
Enclosure 2

has been entered into  
the record as

Appellate Exhibit 178,  
Enclosure 2

Appellate Exhibit 246,  
Enclosure 4  
has been entered into  
the record as  
Prosecution Exhibit 141

UNCLASSIFIED//FOUO

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

)  
)  
) **Prosecution Motion**  
) **For Preliminary Determination of**  
) **Admissibility of Evidence**  
) **(Computer-Generated Records)**

) **Enclosures 5-6**

) **3 August 2012**

*See Attached CD*

UNCLASSIFIED//FOUO

## ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. The records were made by the regularly conducted activity as a regular practice; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

OSC log files, containing the following logs, with the following date ranges:

bmanning_distinct_export_with_classification.xls	6-Nov-09 - 9-Nov-10
bradass87_distinct_export_with_classification.xls	20-Feb-10 - 17-Apr-10
bradass87_sum_export_with_classification.xls	No date range

OSC user information files entitled:

Opensource.gov-bmanning.pdf  
Opensource.gov-bradass87.pdf

Organization: Central Intelligence Agency

Signature *Maxwell Allen*

Date

*6/29/2012*

Print or Type Name

*Maxwell Allen*

Title

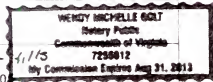
*DBA/  
Owen*

Business Telephone

*865-216-2433*

Business Address

*12020 Switzer  
Washington, DC 20501*



Subscribed and sworn to before a notary public, this *29* day of *June*, 2012.

Notary Public

*Wendy M Golt*

My commission expires on:

*8/31/2013*

## ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(1), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities.
2. The records were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters.
3. The records were kept in the course of regularly conducted business activity.
4. The records were made by the regularly conducted activity as a regular practice, and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

OSD log files - spanning the following logs, with the following date ranges:

branslog67 -branslog67 export, with classification.xls	04-Nov-10 - 03-Nov-11
branslog67 -branslog67 export, with classification.xls	20-Feb-10 - 17-Apr-10
branslog67 -branslog67 export, with classification.xls	No date range

OSD user information files attached:

Operationslog67-branslog67.pdf  
 Operationslog67-branslog67.pdf

Organization: Central Intelligence Agency

Signature

Date

Print or Type Name

Title

Business Telephone

Business Address

20300 S. ...  
 Washington, DC 20305

Subscribed and sworn to before a notary public, this 11 day of May, 2011.

Notary Public

My commission expires on:

Appellate Exhibit 246  
Enclosures 5-6  
(Attachment)

have been entered into  
the record as a CD/DVD  
and will be maintained  
with the original  
Record of Trial



UNITED STATES OF AMERICA

 $\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Prosecution Motion  
For Preliminary Determination of  
Admissibility of Evidence  
(Computer-Generated Records)**

**Enclosures 5-6**

3 August 2012

*See Attached CD*

UNCLASSIFIED//FOUO

## ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(11), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;
2. The records were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of these matters;
3. The records were kept in the course of regularly conducted business activity;
4. The records were made by the regularly conducted activity as a regular practice; and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

OSC log files, containing the following logs, with the following date ranges:

bmaning_distinct_export_with classification.xls	6-Nov-09 - 9-Nov-10
bradass87_distinct_export_with classification.xls	20-Feb-10 - 17-Apr-10
bradass87_sum_export_with classification.xls	No date range

OSC user information files entitled:

Opensource.gov-bmaning.pdf  
Opensource.gov-bradass87.pdf

Organization: Central Intelligence Agency

Signature <i>Maxwell Allen</i>	Date <i>6/29/2012</i>
Print or Type Name <i>Maxwell Allen</i>	Title <i>DBA/ Owen</i>
Business Telephone <i>865-216-2433</i>	Business Address <i>12020 Seward Washington, DC 2050</i>
Subscribed and sworn to before a notary public, this <i>29</i> day of <i>June</i> , 20 <i>12</i> .	
Notary Public <i>Wendy Michelle Golt</i>	My commission expires on: <i>8/31/2013</i>



## ATTESTATION CERTIFICATE

This document is intended to meet the requirements set forth in Military Rules of Evidence Rule 902(f)(1), addressing certified records of regularly conducted activity.

I swear or affirm that each of the following is true regarding the attached records, to the best of my knowledge and belief:

1. I am the custodian of these records, or I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities.
2. The records were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters.
3. The records were kept in the course of regularly conducted business activity.
4. The records were made by the regularly conducted activity as a regular practice, and
5. The records are a true, accurate, and complete copy of the original documents.

List of attached records:

OSCI log files, containing the following logs, with the following date ranges:

bradass67_diffract_export_with_classification.xls	04-Nov-00 - 03-Nov-10
bradass67_diffract_export_with_classification.xls	20-Feb-10 - 17-Apr-10
bradass67_sun_export_with_classification.xls	No date range

OSCI user information files attached:

Open-source.gov-bradass67.pdf  
 Open-source.gov-bradass67.pdf

Organization: Central Intelligence Agency

Signature

Date

Print or Type Name

Title

Business Telephone

Business Address

Washington, DC 20505



Subscribed and sworn to before a notary public, this 1 day of 11, 2011.

Notary Public

My commission expires on:

Appellate Exhibit 246  
Enclosures 5-6  
(Attachment)

have been entered into  
the record as a CD/DVD  
and will be maintained  
with the original  
Record of Trial

Appellate Exhibit 246,  
Enclosure 7  
has been entered into  
the record as  
Prosecution Exhibit 140

Appellate Exhibit 246,  
Enclosure 8  
has been entered into  
the record as  
Prosecution Exhibit 61

Appellate Exhibit 246,  
Enclosure 9  
has been entered into  
the record as  
Prosecution Exhibit 62

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

)  
)  
) **DEFENSE RESPONSE TO**  
) **GOVERNMENT MOTION FOR**  
) **PRELIMINARY**  
) **DETERMINATION OF**  
) **ADMISSIBILITY OF EVIDENCE**  
) **(COMPUTER-GENERATED**  
) **RECORDS)**

) DATED: 17 AUGUST 2012  
)

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, moves this court to deny the Government's motion for a preliminary determination as to the admissibility of computer-generated evidence.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Government has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were referred on 3 February 2012.



## WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion.

## LEGAL AUTHORITY AND ARGUMENT

6. The Defense objects to the admission of the Government's Enclosures to its Motion for Preliminary Determination on Admissibility of Evidence dated 3 August 2012 because they are testimonial hearsay falling outside the scope of M.R.Es 803(6) and 902(11).

I. The Enclosures Are Hearsay Because They Contain Statements by the Computer User

7. R.C.M. 801(a) defines a statement as either "an oral or written assertion" or "nonverbal conduct of a person." Here, the Enclosures in question contain the statements of a computer user(s). That is, the Enclosures contain written assertions and nonverbal conduct by the user(s) of various computers.

8. The Government relies heavily on the decision in *U.S. v. Blazier*, 69 M.J. 218 (C.A.A.F. 2010) to suggest that the Enclosures in question are machine-generated. There, the court was concerned with the amount of human intervention in the creation of the record. *Id.* at 224. Although, the Government noted this in its motion, it failed to actually address the amount of human intervention involved in the creation of each record it seeks to admit. Rather, the Government simply made the blanket assertion that the Enclosures are computer-generated. It would seem the Government is arguing that because the records were kept on a computer, document computer activity and a computer was used to print the record, the record must be "computer-generated." Following the Government's rationale to its logical conclusion would leave ridiculous results. For example, a printed copy of this motion would not amount to hearsay because it was created using a computer, stored on a computer and printed using a computer; never mind the fact that a user had to input all the data that the computer "generates."

9. The Enclosures the Government seeks to admit involve significant human intervention and cannot be considered "wholly machine-generated." Unlike the urinalysis reports the Government attempts to analogize, here the data the Government seeks to pre-admit amounts to a statement by the computer user. With a urinalysis report, the computer creates a record out of whole cloth; it takes a sample, analyzes it and produces data. Here, the Enclosures are records of searches actually typed in by a user of the computer. But for the user typing the exact phrases, names and terms, and conducting the various actions documented<sup>1</sup>, the record the Government seeks to admit would not exist. Thus, it is clear that the amount of human intervention in the creation of these records is significant. It must follow that the records containing those exact phrases, names and terms are a statement by the user.

10. Because the Enclosures contain out of court statements from the user(s) of various computers and the Government seeks to offer them for the truth of the matter asserted, the

---

<sup>1</sup> Be it opening a file, creating a file, visiting a website, typing a search or any other user conduct that is memorialized in the Enclosures.

Government must point to a hearsay exception. Absent such an exception the Enclosures should not be admitted.

## II. The Enclosures Are Testimonial Hearsay Pursuant to *Crawford*

11. Additionally, the reports themselves are testimonial hearsay. M.R.E. 803(6) establishes an exception to the general rule against hearsay where records are kept in the course of “regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation., all as shown by the testimony of the custodian or other qualified witness, or be certification that complies with M.R.E. 902(11).”

12. Despite this exception to the prohibition against hearsay, a business record must also satisfy the 6th Amendment’s Confrontation Clause. The Court in *Crawford v. Washington* established that where testimonial hearsay is at issue the Confrontation Clause is only satisfied if the Accused is afforded an opportunity for cross-examination. 541 U.S. 36, 59 (2004). The *Crawford* Court defined testimonial hearsay further as “statements that were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial.” *Id.* at 51.

13. C.A.A.F.’s ruling in *U.S. v. Rankin*, 64 M.J. 348 (2007), is instructive on what amounts to testimonial hearsay in the military context. There, the court established a three-part test for identifying testimonial hearsay:

(1) was the statement at issue elicited by or made in response to law enforcement or prosecutorial inquiry; (2) did the statement involve more than a routine and objective cataloging of unambiguous factual matters; and (3) was the primary purpose for making, or eliciting, the statement the production of evidence with an eye toward trial.

*Id.* at 352.

14. The C.A.A.F. in *U.S. v. Harcrow*, applied the Rankin factors when considering whether laboratory reports created upon request by the county sheriff were testimonial. 66 M.J. 154 (2008). In considering the Confrontation Clause issue, the court noted, “[h]ere the laboratory tests were specifically requested by law enforcement and the information relayed on the laboratory reports pertained to items seized during the arrest of an identified ‘suspect.’” *Id.* at 159. The court further held, “lab results or other types of routine records may become testimonial where a defendant is already under investigation, and where the testing is initiated by the prosecution to discover incriminating evidence.” *Id.* (quoting *U.S. v. Magyari*, 63 M.J. 123 (2006)).

15. Similarly, the Coast Guard Court of Criminal Appeals applied the Rankin Factors in determining statements in a cover memorandum were testimonial. *U.S. v. Byrne*, 70 M.J. 611 (2011). In *Byrne*, the court found the Confrontation Clause had been violated when a “Laboratory Document Packet” regarding an alleged positive urinalysis was admitted over defense objection. In weighing the *Rankin* factors the Court noted, “we find the statements in the

cover memorandum were made in response to a request for a litigation packet, which clearly indicates that a court-martial is being contemplated, and, thus, the memorandum was prepared in response to a prosecutorial inquiry.” *Id.* at 614.

16. In the case at hand, the Government seeks to introduce Enclosures that are testimonial in nature. Specifically, the Government’s Enclosures fall outside the scope of 803(6) and 902(11) because they were made in preparation for trial. In each instance, the record contained in the various Enclosures was created at the behest of the Government. That is, they did not exist in the present form until the Government requested them with an eye towards trial. Because they were made in preparation for trial they are testimonial in nature and, pursuant to *Rankin* and the 6th Amendment, should not be admitted at this time.

#### CONCLUSION

17. Based on the above, the Defense requests that the Court deny, in part, the Government’s motion to pre-admit evidence under R.C.M. 902(11).

Respectfully submitted,



JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Government Motion  
to Take Judicial Notice

3 August 2012

RELIEF SOUGHT

The United States in the above-captioned case requests this Court take judicial notice of the following adjudicative facts:

- (1) Army Regulation (AR) 25-2, paragraphs 1-4, 1-5, 3-3, 4-5, 4-16, 4-17, and figure B-1
- (2) AR 380-5, paragraphs 1-20, 1-21, 1-22; Chapter 2; Chapter 4 (Section I); Chapter 5 (Sections I and V); paragraphs 6-1, 6-2, 6-3, 7-4, 8-3, and 8-12;
- (3) AR 530-1, paragraphs 1-5, 1-6, 1-7, and 2-1;
- (4) 18 U.S.C. § 641;
- (5) 18 U.S.C. § 793(e);
- (6) 18 U.S.C. § 1030 (a)(1);
- (7) Executive Order 13526; and
- (8) Authorization for Use of Military Force

BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. RCM 905(c)(2). The United States has the burden of persuasion as the moving party.

FACTS

The accused is charged with giving intelligence to the enemy, in violation of Article 104, Uniform Code of Military Justice (UCMJ). The accused is also charged with eight specifications alleging misconduct in violation of 18 U.S.C. § 793(e), five specifications alleging misconduct in violation of 18 U.S.C. § 641, two specifications alleging misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications alleging misconduct in violation of Article 92, UCMJ, and one specification alleging misconduct prejudicial to good order and discipline and service discrediting. See Charge Sheet.

WITNESSES/EVIDENCE

The United States requests this Court consider the referred charge sheet in support of its motion, as well as Enclosures 1-8.

APPELLATE EXHIBIT 248  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

## LEGAL AUTHORITY AND ARGUMENT

A judicially noticed fact must be “adjudicative” and “must be one not subject to reasonable dispute in that it is either (1) generally known universally, locally, or in the area pertinent to the event or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Military Rule of Evidence (MRE) 201.

### A. Army Regulations

Army Regulation 25-2, dated 24 October 2007, provides the Army's Information Assurance (IA) policy, mandates, roles, responsibilities, and procedures for implementing the Army IA program. Paragraphs 1-4 and 1-5 address the purpose behind the Army IA program and provide an overview of the program. Paragraph 3-3 addresses the roles and responsibilities of IA support personnel. Paragraphs 4-5(a)(3) and 4-5(a)(4) discuss activities that are specifically prohibited by any authorized user on a Government-provided Information System or connection. Paragraph 4-16 addresses information systems media protection requirements and states that Army personnel will not transmit classified information over any communication systems unless using approved security procedures and practices. Paragraph 4-17 addresses the proper procedures for labeling, marking, and controlling information systems media. Figure B-1 is a template Acceptable Use Policy. The Accused is charged with attempting to bypass network or information systems security mechanisms, adding unauthorized software to a Secret Internet Protocol Router Network computer, and using an information system in a manner other than its intended purpose.

The existence of AR 25-2, dated 24 October 2007, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to a source whose accuracy cannot be reasonably questioned.

The fact that AR 25-2, dated 24 October 2007, was in effect between 1 November 2009 and 27 May 2010, the time period in which the accused was alleged to have committed the charged misconduct in this case, is generally known and capable of accurate and ready determination by resort to the AR whose accuracy cannot be reasonably questioned.

The fact that the accused had a duty to obey AR 25-2 is a fact not subject to reasonable dispute. AR 25-2 applies to military personnel of the Active Army and applies to all users in all environments. AR 25-2, paragraph 1-5(j) states that “military and civilian personnel may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DOD and Army policies and procedures.”

AR 380-5 establishes policies for classification, downgrading, declassification, and safeguarding of information requiring protection in the interest of national security. Paragraphs 1-20, 1-21, and 1-22, discuss the corrective actions and sanctions that are taken when a violation of this regulation has occurred. Chapter 2 discusses the role of Original Classification Authorities, the classification process, derivative classification, security classification guides, and classification of non-government information. Chapter 4, Section I, discusses the proper procedures for marking documents. Chapter 5, Section I, discusses the proper handling of controlled unclassified information which also requires protection in order to prevent damage to the national security. Chapter 5, Section V, addresses sensitive information and discusses the proper procedures for

marking and handling this type of material. Paragraph 6-1 discusses the responsibilities of Department of the Army (DA) personnel in accessing classified information. Paragraph 6-2 discusses nondisclosure agreements and states that DA personnel will receive a briefing regarding their responsibilities in protecting classified information and will sign a classified information nondisclosure agreement (NDA). Paragraph 6-3 discusses the signing and filing of the NDA. Paragraph 7-4, discusses the standards for storage of classified information, and states that classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a locked security container, vault, room, or area, pursuant to the level of classification. Paragraph 8-3, discusses the proper methods for transporting and transmitting "SECRET" information. Paragraph 8-12, discusses the general provisions for escorting or hand carrying classified material. The accused is charged with, *inter alia*, improperly handling and storing classified material.

The existence of AR 380-5, dated 29 September 2000, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to a source whose accuracy cannot be reasonably questioned.

The fact that AR 380-5, dated 29 September 2000, was in effect between 1 November 2009 and 27 May 2010, the time period in which the accused was alleged to have committed the charged misconduct in this case, is generally known and capable of accurate and ready determination by resort to the AR whose accuracy cannot be reasonably questioned.

The fact that the accused had a duty to obey AR 380-5 is a fact not subject to reasonable dispute. AR 380-5 applies to military personnel of the Active Army and applies to all users in all environments. AR 380-5, paragraph 1-21(a) subjects DA personnel to sanctions if they "knowingly, willfully, or negligently" do any of the following: "(1) Disclose classified or sensitive information to unauthorized persons, (2) Classify or continue the classification of information in violation of this regulation, (3) Violate any other provision of this regulation."

AR 530-1, dated 19 April 2007, addresses Army policy on Operations Security (OPSEC) program development, provides details on the OPSEC planning process, and outlines the OPSEC review, assessment, and survey. Paragraph 1-5 discusses the definition of OPSEC, critical information, sensitive information, and OPSEC compromise. Paragraph 1-6 discusses the requirement of each DOD component to have an OPSEC program and the purpose behind the requirement. Paragraph 1-7 discusses the application of OPSEC. Paragraph 2-1 addresses Army personnel operations security responsibility and the results of failure to implement OPSEC measures.

The existence of AR 530-1, dated 19 April 2007, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to a source whose accuracy cannot be reasonably questioned.

The fact that AR 530-1, dated 19 April 2007, was in effect between 1 November 2009 and 27 May 2010, the time period in which the accused was alleged to have committed the charged misconduct in this case, is generally known and capable of accurate and ready determination by resort to the AR whose accuracy cannot be reasonably questioned.

The fact that the Accused had a duty to obey AR 530-1 is a fact not subject to reasonable dispute. AR 530-1 applies to military personnel of the Active Army and applies during all phases of operations. Army Regulation 530-1, paragraph 2-1(b)(2) states "a failure to comply with these orders, directives, or policies may be punished as violations of a lawful order under Article 92 of the UCMJ."

#### B. Executive Order

Executive Order 13526 addresses classified national security information by prescribing a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. The order authorizes information to be classified when it concerns foreign relations or foreign activities of the United States.

The existence of Executive Order 13526, dated 29 December 2009, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to the White House website at <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>, a source whose accuracy cannot be reasonably questioned.

The fact that Executive Order 13526, dated 29 December 2009, was in effect at the time the Accused was charged with compromising classified material, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to the White House website at <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>, a source whose accuracy cannot be reasonably questioned.

#### C. Federal Statutes

The existence of 18 U.S.C. § 641 is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to Title 18, United States Code, a source whose accuracy cannot be reasonably questioned.

The fact that 18 U.S.C. § 641 was in effect at the time the accused was charged with stealing or converting government property is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to Title 18, United States Code, a source whose accuracy cannot be reasonably questioned.

The existence of 18 U.S.C. § 793(e) is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to Title 18, United States Code, a source whose accuracy cannot be reasonably questioned.

The fact that 18 U.S.C. § 793(e) was in effect at the time the accused was charged with transmitting national defense information is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to Title 18, United States Code, a source whose accuracy cannot be reasonably questioned.

The existence of 18 U.S.C. § 1030(a)(1) is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to Title 18, United States Code, a source whose accuracy cannot be reasonably questioned.

The fact that 18 U.S.C. § 1030(a)(1) was in effect at the time the accused was charged with exceeding authorized access on a Secret Internet Protocol Router Network computer is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to Title 18, United States Code, a source whose accuracy cannot be reasonably questioned.

#### D. Joint Resolution


The Authorization for Use of Military Force authorized the President to “use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations, or persons.”

The existence of the Authorization for Use of Military Force, signed into law 18 September 2001, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to the U.S. Government Printing Office website at <http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm>, a source whose accuracy cannot be reasonably questioned.

The fact that the Authorization for Use of Military Force, signed into law 18 September 2001, was in effect at the time the accused was charged a violation of Article 104, UCMJ, is a fact not subject to reasonable dispute. This fact is generally known and capable of accurate and ready determination by resort to the U.S. Government Printing Office website at <http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm>, a source whose accuracy cannot be reasonably questioned.

#### CONCLUSION

For the reasons stated above, the United States requests the Court take judicial notice of the existence and the content of the above-mentioned portions of the Army Regulations, the Executive Order, the Federal Statutes, and the Joint Resolution, as they meet all the requirements of MRE 201.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel



I certify that I served or caused to be served a true copy of the above on Defense Counsel via electronic mail, on 3 August 2012.

  
JODEAN MORROW  
CPT, JA

Assistant Trial Counsel

8 Encls

1. AR 25-2, paragraphs 1-4, 1-5, 3-3, 4-5, 4-16, 4-17, and figure B-1
2. AR 380-5, paragraphs 1-20, 1-21, 1-22; Chapter 2, Chapter 4 (Section I); Chapter 5 (Sections I and V); paragraphs 6-1, 6-2, 6-3, 7-4, 8-3, and 8-12
3. AR 530-1, paragraphs 1-5, 1-6, 1-7, and 2-1
4. 18 U.S.C. § 641
5. 18 U.S.C. § 793(e)
6. 18 U.S.C. § 1030 (a)(1)
7. Executive Order 13526
8. Authorization for Use of Military Force

)  
 )  
 )  
 )  
 )  
 )  
 )  
 )

**V.**

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

### Government Motion to Take Judicial Notice

**Enclosure 1**

3 August 2012

Information Management

# Information Assurance

**Rapid Action Revision (RAR) Issue Date: 23 March 2009**

Headquarters  
Department of the Army  
Washington, DC  
24 October 2007

**UNCLASSIFIED**

## **Chapter 1**

### **Introduction**

#### **1-1. Purpose**

This regulation establishes information assurance (IA) policy, roles, and responsibilities. It assigns responsibilities for all Headquarters, Department of the Army (HQDA) staff, commanders, directors, IA personnel, users, and developers for achieving acceptable levels of IA in the engineering, implementation, operation, and maintenance (EIO&M) for all information systems (ISs) across the U.S. Army Enterprise Infrastructure (AEI).

#### **1-2. References**

Required and related publications and prescribed and referenced forms are listed in appendix A.

#### **1-3. Explanation of abbreviations and terms**

Abbreviations and special terms used in this regulation are explained in the glossary.

#### **1-4. Army Information Assurance Program**

a. The Army Information Assurance Program (AIAP) is a unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by ISs, and is established to consolidate and focus Army efforts in securing that information, including its associated systems and resources, to increase the level of trust of this information and the originating source. The AIAP will secure ISs through IA requirements, and does not extend access privileges to special access programs (SAPs), classified, or compartmentalized data; neither does it circumvent need-to-know requirements of the data or information transmitted.

b. The AIAP is designed to achieve the most effective and economical policy possible for all ISs using the risk management approach for implementing security safeguards. To attain an acceptable level of risk, a combination of staff and field actions is necessary to develop local policy and guidance, identify threats, problems and requirements, and adequately plan for the required resources.

c. Information systems exhibit inherent security vulnerabilities. Cost-effective, timely, and proactive IA measures and corrective actions will be established and implemented to mitigate risks before exploitation and to protect against vulnerabilities and threats once they have been identified.

(1) Measures taken to attain IA objectives will be commensurate with the importance of the operations to mission accomplishment, the sensitivity or criticality of the information being processed, and the relative risks (the combination of threats, vulnerabilities, countermeasures, and mission impact) to the system. Implementation of an IA operational baseline will be an incremental process of protecting critical assets or data first, and then building upon those levels of protection and trust across the enclave.

(2) Statements of security requirements will be included in the earliest phases (for example, mission needs statements, operational requirements document, capstone requirement document) of the system acquisition, contracting, and development life cycles.

d. An operationally focused IA program requires the implementation of innovative approaches. Through the use of IA best business practices (BBPs) the best ideas, concepts, and methodologies acquired from industry and Army resources will be used to define specific standards, measures, practices, or procedures necessary to meet rapidly changing technology or IA requirements in support of Army policy requirements. IA BBPs allow rapid transitional implementation of IA initiatives to integrate, use, improve, or modify technological or procedural changes as required by policy. BBPs are located at <https://informationassurance.us.army.mil>.

e. The elements of the Defense in Depth (DiD) strategy focus on three areas: people, operations, and defense of the environment (the latter of which encompasses the computing environment, the networks, the enclave boundaries, and the supporting infrastructure).

f. The AIAP is not a stand-alone program, but incorporates related functions from other standards or policies such as; operations security (OPSEC), communications security (COMSEC), transmission security (TRANSEC), information security (INFOSEC), personnel security, and physical security to achieve IA requirements.

g. Failure to implement proactive or corrective IA security measures, guidance, policy, or procedures may prevent system or enclave accreditation, installation, or operation and may increase system vulnerability to foreign and domestic computer network operation (CNO) activities designed to deny service, compromise information, or permit unauthorized access to sensitive information. IA or network personnel may block access to ISs that reflect poor IA security practices or fail to implement corrective measures.

#### **1-5. Overview**

a. The AIAP applies to ISs including, but not limited to, computers, processors, devices, or environments (operating in a prototype, test bed, stand-alone, integrated, embedded, or networked configuration) that store, process, access, or transmit data, including unclassified, sensitive (formerly known as sensitive but unclassified (SBU)), and classified data, with or without handling codes and caveats. ISs used for teleworking, telecommuting, or similar initiatives; contractor owned or operated ISs; ISs obtained with non-appropriated funds; automated tactical systems (ATSS);

automated weapons systems (AWSs); distributed computing environments (DCEs); and systems processing intelligence information are required to adhere to the provisions of this regulation.

b. Commanders of activities requiring limited access by any local foreign national (FN) officials or personnel (including information technology (IT) positions) will follow the provisions of this regulation.

c. This regulation applies equally to the operation, safeguarding, and integrity of the infrastructures (for example, power, water, air conditioning), including the environment in which the IS operates.

d. While no regulation or policy on security measures can ever provide a 100 percent solution, implementation of the concepts, procedures, and recommendations in this regulation will drastically reduce the manageability requirements of assets, and minimize the effects of unauthorized access or loss. The cornerstone philosophy of IA is to design, implement, and secure access, data, ISs, and data repositories; increase trust and trusted relationships; employ technical and operational security mechanisms; deny all unauthorized accesses; and permit necessary exceptions to support Army, DOD, and Joint interagency and multinational (JIM) tactical and sustaining-base operations.

e. Army information constitutes an asset vital to the effective performance of our national security roles. While all communication systems are vulnerable to some degree, the ready availability of low-cost IT, freely distributed attack tools, increased system connectivity and asset distribution, and attack-standoff capabilities make computer network attacks (CNAs) an attractive option to our adversaries. Information Assurance capabilities and actions protect and defend network availability, protect data integrity, and provide the ability to implement effective computer network defense (CND). Management of Army information is imperative so that its confidentiality, integrity, availability, and non-repudiation can be ensured, and that users of that data can be properly identified and authenticated.

f. The AEI architecture requires the establishment, verification, and maintenance of trusted enclaves, trusted connectivity, and trusted information and information sources along with the capability to access and distribute that information by leveraging technology and capabilities to amplify that trust.

g. To accomplish these foundational objectives, this regulation establishes requirements as follows:

- (1) Provides administrative and systems security requirements, including those for interconnected systems.
  - (2) Defines and mandates the use of risk assessments.
  - (3) Defines and mandates the DID strategy.
  - (4) Promotes the use of efficient procedures and cost-effective, computer-based security features and assurances.
  - (5) Describes the roles and responsibilities of the individuals who constitute the IA security community and its system users, and outlines training and certification requirements.
  - (6) Requires a life cycle management approach to implementing IA requirements.
  - (7) Introduces the concepts of mission assurance category, levels of confidentiality, and levels of robustness of information.
  - (8) Implements DODD 8500.1, DODI 8500.2, and Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 to align IA goals and requirements to support the DOD Information Management Strategic Plan.
  - (9) Mandates procedures to document the status of accreditations for all ISs fielded by DOD organizations, Army chartered program managers (PMs), and HQDA staff proponents.
  - (10) Mandates that DOD and Army-level designated approving authorities (DAAs) meet the system accreditation requirements of this regulation before fielding or testing any system that requires connection to an Army network.
  - (11) Requires the implementation of a configuration management (CM) process.
  - (12) Describes the Continuity of Operations Plan (COOP).
  - (13) Provides the foundation for the Networkability Certification Program in AR 25-1.
- h. Other policies, procedures, or directives also govern certain systems. In the event of conflicts among these policies, procedures, or directives, the more stringent requirement will take precedence. When the most stringent policy cannot be determined, the affected Army component will submit a request for a policy decision through their supporting regional chief information officers/functional chief information officers (RCIOs/FCIOs) to the Chief Information Officer/G-6 (CIO/G-6).
- i. The mention of commercial products in this regulation does not imply endorsement by either DOD or the Army.
- j. Military and civilian personnel may be subject to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring implementation of DOD and Army policies and procedures. Violations are identified in bolded text included in the following paragraphs 3-3, 4-5, 4-6, 4-12, 4-13, 4-16, 4-20, and 6-5.

k. These provisions may be punished as violations as follows:

- (1) Sanctions for civilian personnel may include, but are not limited to, some or all of the following administrative actions: oral or written warning or reprimand; adverse performance evaluation; suspension with or without pay; loss or suspension of access to IS or networks, and classified material and programs; any other administrative sanctions authorized by contract or agreement; and/or dismissal from employment. Sanctions for civilians may also include prosecution in U.S. District Court or other courts and any sentences awarded pursuant to such prosecution. Sanctions may be awarded only by civilian managers or military officials who have authority to impose the specific sanction(s) proposed.

- (10) Perform required monitoring of network resources per this regulation.
- (11) Ensure the use of Army approved IA products from the IA Approved Products List.
- (12) Implement IA and IAVM reporting and compliance procedures as set out in CJCSM 6510.01.
- (13) Analyze and maintain network audit data.
- (14) Ensure adequate network connectivity by making proper decisions concerning levels of confidentiality and robustness for the system.

*f. IASO.* The commander or manager/director of the activity responsible for the ISs will appoint an IASO for each IS or group of ISs. The same IASO may be appointed for multiple ISs. The IASO position will be designated IT-I, IT-II, or IT-III. A contractor may not fill MSC, installation, or post IASO positions at IT-I, if created. The IASO must be IA certified and maintain his or her certification. Appoint pre-deployment or operational IASOs for developmental systems with the applicable responsibilities. DOD uses the term IAO for IASO responsibilities. All IASOs will—

- (1) Enforce IA policy, guidance, and training requirements per this regulation and identified BBPs.
- (2) Ensure implementation of IAVM dissemination, reporting, and compliance procedures.
- (3) Ensure all users meet the requisite favorable security investigations, clearances, authorization, need-to-know, and security responsibilities before granting access to the IS.
- (4) Ensure users receive initial and annual IA awareness training.
- (5) Ensure log files and audits are maintained and reviewed for all systems and that authentication (for example, password) policies are audited for compliance.
- (6) Prepare, distribute, and maintain plans, instructions, and SOPs concerning system security.
- (7) Review and evaluate the effects on security of system changes, including interfaces with other ISs and document all changes.
- (8) Ensure that all ISs within their area of responsibility are certified, accredited and reaccredited.
- (9) Maintain and document CM for IS software (including IS warning banners) and hardware.
- (10) Pre-deployment or operational IASOs will ensure system recovery processes are monitored and that security features and procedures are properly restored.
- (11) Pre-deployment or operational IASOs will maintain current software licenses and ensure security related documentation is current and accessible to properly authorized individuals.
- (12) Tenant IASOs will support and assist tenant IAMs (or the installation IAM if no tenant IAM exists).
- (13) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.

### 3-3. Information assurance support personnel

In addition to the above described IA structure, other personnel have crucial responsibilities.

*a. System or network administrators.* System administrators (SAs) and network administrators (NAs) must be designated IT-I, IT-II, or IT-III (see para 4-14). Each SA/NA must be trained, experienced, IA certified, and currently certified on the ISs that they are required to maintain. The SA/NA should be a U.S. citizen and must hold a U.S. Government security clearance and local access approvals commensurate with the level of information processed on the system or network. SA/NA responsibilities include, but are not limited to, implementing the AIAP within their command, installation, or activity. SA/NAs will be designed on appointment orders and will—

- (1) Enforce the IS security guidance policies as provided by the IAM and perform IASO duties if an IASO has not been appointed.
- (2) Enforce system access, operation, maintenance, and disposition requirements.
- (3) Ensure that personnel meet required security investigation, clearance, authorization, mission requirement, and supervisory approval before granting access to the IS.
- (4) Report security violations and incidents to the servicing RCERT in accordance with Section VIII, Incident and Intrusion Reporting.
- (5) Conduct required IAVM scanning and vulnerability assessments with approved software as authorized by their IAM/IASO. SAs/NAs are not limited to only IAVM scanning, but should be conducting comprehensive network assessments of their networks as authorized.
- (6) Ensure CM includes all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, and service packs with IAM or IAPM approval.
- (7) Ensure any system changes resulting from updating or patching are reported to the IAM/IASO.
- (8) Record IAVM compliance in the Asset and Vulnerability Tracking Resource (A&VTR) database.
- (9) Maintain current anti-virus (AV) engines and definitions on all ISs.
- (10) Review and verify currency of user accounts, accesses, and logins. Remove departing users' accounts before departure. Terminate inactive accounts verified as no longer required that exceed 45 days.
- (11) Suspend user accounts for the following types of actions: actions that knowingly threaten, damage, or harm the IS, network or communications security; revocation, suspension, or denial of security clearance or interim security clearance investigations; or unauthorized use of IS and networks per para 4-5.

(12) Remove or disable all default, guest, and service accounts in ISs or network devices, and rename administrative accounts as applicable.

(13) **Maintain and use at least 2 separate accounts for access to network resources, 1 for their privileged level access and a separate general user, non-privileged level account for routine procedures.**

(14) Review IS and network audit logs and log files, and report anomalous or suspicious information in accordance with Section VIII, Incident and Intrusion Reporting.

(15) Monitor IS performance to ensure that recovery processes, security features, and procedures are properly restored after an IS has been rebooted.

(16) Monitor IS performance to ensure that processes, security features, and operating system configurations are unaltered.

(17) Perform equipment custodian duties as necessary.

(18) Notify the IAM or IAPM when a system no longer processes sensitive or classified information, or when changes occur that might affect C&A, to obtain disposition or resolution instructions.

(19) Ensure CM for security-relevant IS software (including IS warning banners) and hardware is maintained and documented.

(20) Implement and test IS and data backup procedures for integrity.

(21) Prohibit attempts to strain or test security mechanisms or to perform network-line or keystroke monitoring without authorization.

(22) Establish audit trails, conduct reviews, and create archives as directed by the IAM.

(23) Will sign a Privileged-level Access Agreement (PAA) and a Non-Disclosure Agreement (NDA) as a prerequisite to maintaining their positions. Reference the IA BBP on PAA; AUP (<https://informationassurance.us.army.mil>).

*b. Data owners.* Data owners will, at a minimum, provide guidance or feedback to the System Owner (SO) concerning—

(1) The confidentiality of information under the data owner's purview.

(2) The DIACAP team's decision regarding the level of classification, confidentiality, integrity, availability, encryption, and protection requirements for the data at rest or in transit.

(3) Specific requirements for managing the owner's data (for example, incident response, information contamination to other system/media, and unique audit requirements).

(4) Whether FNs may access ISs accredited under this regulation. Access must be consistent with DOD, DA, and DIA governing directives (for example, AR 380-10 and DCIDs 1/7 and 5/6).

*c. General users.* Use of Government IS and access to Government networks is a revocable privilege, not a right. Users are the foundation of the DiD strategy and their actions affect the most vulnerable portion of the AEI. Users must have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Users will—

(1) **Comply with the command's AUP for Government owned ISs and sign an AUP prior to or upon account activation.**

(2) Complete initial and/or annual IA training as defined in the IA training BBP (<https://informationassurance.us.army.mil>).

(3) Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them with a valid need to know.

(4) Protect ISs and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

(5) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

(6) **Obtain prior approval for the use of any media (for example, USB, CD-ROM, floppy disk) from the SA/IAM.**

(7) **Scan all files, attachments, and media with an approved and installed AV product before opening a file or attachment or introducing media into the IS.**

(8) Report all known or suspected spam, chain letters, and violations of acceptable use to the SA, IAM, or IASO.

(9) Immediately stop using an infected IS; and report suspicious, erratic, or anomalous IS operations, and missing or added files, services, or programs to the SA/IASO in accordance with local policy.

(10) **Not disclose their individual account password or pass-phrase authenticators.**

(11) **Invoke password-protected screen locks on your workstation after not more than 15 minutes of non-use or inactivity.**

(12) **Logoff ISs at the end of each workday.**

(13) **Access only that data, control information, software, hardware, and firmware for which the user is authorized access.**

(14) Access only that data that they are authorized or have a need to know.

(15) Assume only authorized roles and privileges as assigned.

(16) Users authorized Government-provided IA products (for example, AV or personal firewalls) will be encouraged to install and update these products on their personal systems and may be required to do so as directed by the DAA and documented in the C&A package for any approved remote access.

*d. COMSEC custodians and inspecting personnel.* Execute responsibilities as required per this regulation and AR 380-40.

*e. TEMPEST personnel.* Execute responsibilities as required in AR 381-14.

*f. Intelligence personnel.* Senior intelligence officers (SIOs) or command intelligence officers (DCSINT/G2s/S2s) will—

(1) Ensure the command statement of intelligence interest (SII) (AR 381-10 and AR 381-20) registers requirements for the receipt of validated intelligence adversely affecting the integrity and reliability of ISs.

(2) Provide assistance in the identification of threat factors affecting the risk management approach for implementing security safeguards.

*g. Force protection officers.* Execute responsibilities as required by AR 525-13.

*h. Information operations officers.* Execute responsibilities as required by FM 3-13.

*i. OPSEC officers.* The primary OPSEC vulnerability is information made publicly accessible through Web sites and Web-enabled applications. Commanders and Directors will develop and implement an OPSEC review plan as part of their inspection programs. All content placed on a Web site will be reviewed for OPSEC sensitive information. Additionally, execute responsibilities as required per AR 530-1.

*j. Public affairs officers (PAOs).* Execute IA responsibilities as required per this and AR 25-1.

*k. Acquisition officers.* Include IA requirements in the acquisition phases and execute responsibilities as required by DOD 5000.2-R and NSTISSP No. 11.

*l. DOI/MS.* Execute responsibilities per this regulation and AR 25-1.

*m. DAAs (see para 5-8).*

(1) The DAA will—

(a) Be a U.S. citizen.

(b) Hold a U.S. Government security clearance and access approvals commensurate with the level of information processed by the system under his or her jurisdiction.

(c) Be an employee of the U.S. Government and meet the grade requirements identified in paragraph 5-8.

(d) Complete the DAA Basics Computer Based Training prior to performing the duties of DAA.

(e) Request appointment from the CIO/G-6 for IS by name.

(f) Ensure the DAA position is designated as an IT-1, based on the duties assigned and the expected effects on the Army mission.

(g) Meet training and certification requirements in accordance with NSTISSI No. 4012.

(h) The DAA will understand the operational need for the systems and the operational consequences of not operating the systems. The DAA will have an in-depth knowledge of DiD to drive state-of-the-art acquisition, focus a robust training program, and institute executable policy across the IA enterprise.

(2) The DAA will ensure the following as a minimum—

(a) Proper C&A based on systems environment, mission assurance category (MAC) level, confidentiality level, and security safeguards in accordance with this regulation and the Interim DIACAP.

(b) Issue written memo or digitally signed e-mail IA C&A authorization statements (that is, interim approval to operate (IATO), interim authorization to test (IATT), approval to operate (ATO), denial of authorization to operate (DATO)), after receipt of CA recommendation.

(c) Maintain records (including use of IA tools) for all IS C&A activities under his or her purview.

(d) Accomplish roles and responsibilities as outlined in this regulation during each phase of the accreditation process and for each IS as required.

(e) Ensure operational IS security policies are in place for each system, project, program, and organization or site for which the DAA has approval authority.

(f) Incorporate security, C&A, and Networthiness as an element of the life cycle process.

(g) Ensure data owner requirements are met before granting any FN access to the system.

(h) Consider and acknowledge CI and criminal intelligence activities during the C&A process.

(i) Report security-related events to affected parties (for example, data owners, all involved DAAs). DAAs must coordinate with investigative activities (for example, CCIU, RCERT) before making notifications.

(j) Assign written security responsibilities to the individuals reporting directly to the DAA (for example, IAM or an IASO if an IAM does not exist).

(k) Appoint a CA for each IS (or group of ISs) and network.

(l) Ensure CSLA certification of cryptographic applications occurs during the C&A process.

*n. CA Authority and responsibility for certification is vested in the Army FISMA Senior IA Officer (SIAO). The*



Director OIA&C, NETC-EST-I, was appointed FISMA SIAO by the CIO/G-6 and will be the single Army certification authority (see para 5-2).

*o. Agent of the certification authority (ACA).* (See also para 5-9). The Army CA will maintain a list of qualified Government organizations and labs, as Agents of the CA (ACA), to perform the certification activities. The ACAs, funded by the SOs, are available to provide SOs with certification capabilities. Organizations can request appointment as an ACA by following the process in the ACA BPP.

*p. SO.* A Government SO will be identified for each IS used by or in support of the Army. The SO is responsible for ensuring the security of the IS as long as it remains in Army inventory, or until transferred (temporarily or permanently) to another Government person or organization and such transfer is appropriately documented, and provided as an artifact to the accreditation package (see para 5-10).

*q. Host and tenant responsibilities.* Army tenant units or activities must comply with the IA requirements of their parent ACOM/ASCC and their supporting installation. Army and non-Army tenant operations must comply with the host installation's IA policy if they connect to the installation's information infrastructure. Army tenant units or activities and units based in or under operational control (OPCON) of an ACOM/ASCC other than their parent will comply with the IA requirements of both parent and host commands. Address unresolved conflicts of IA policy per this regulation through local command channels and RCI/Os to HQDA, CIO/G-6. Until CIO/G-6 resolves the conflict, the provisions of this regulation will apply, including those pertaining to the use of gateways or information management resources as pathways to connect their ISS. If the non-Army tenant uses any part of the host installation infrastructure, the installation IAM will require the use of CM controls consistent with the installation's information management and CM process. All tenant activities will—

- (1) Identify and coordinate all system upgrades, fieldings, pilots, tests, and operations of new or upgraded systems with the installation IAM, DAA, and DOIM.
- (2) Identify ISS and provide the approved C&A documentation to the installation IAM.
- (3) Identify their security support requirements to the installation IAM and provide technical assistance, as required.
- (4) Identify appropriate IA personnel to the installation IAM.
- (5) Support installation IA efforts and requirements, and identify constraints in sufficient time to permit coordination and preparation of a viable IS security solution.
- (6) Coordinate and conduct vulnerability assessments or compliance scanning, and report completion and results as required.

## **Chapter 4**

### **Information Assurance Policy**

#### **Section I**

##### **General Policy**

#### **4-1. Policy overview**

This chapter provides policy to implement IA requirements developed to respond to the IA challenge, as defined in Public Law, National Security, DOD, and Army directives, policies, and regulations.

*a.* Implement all security analyses, security engineering, and security countermeasures to protect ISS within the framework of risk management and adherence to public laws, DOD directives, and Army regulations.

*b.* Define a security policy and a protection profile for ISS during concept development. Consider security requirements based on these items throughout the IS life cycle.

*c.* The IS developer will ensure the early and continuous involvement of the functional proponent, threat and risk assessors, users, IA personnel, data owners, certification authorities, and DAAs in defining and implementing security requirements of the IS.

*d.* Statements of security requirements will be included in the acquisition and procurement specifications and contracts for ISS, products, and services. Purchases will be in accordance with Army contracting and acquisition guidelines, Blanket Purchase Agreements (BPAs), and IA-approved products. NIST Special Publication 800-64 REV.1 may be referenced for specification, tasks, and clauses that are used in writing contracts. The statements will reflect an initial risk assessment and will specify the required protection level per DODD 8500.1 and DODI 8500.2.

*e.* The ACOMs, ASCCs, DRUs, direct reporting PMs, or functional proponents will not field, and commanders will not accept, systems—

(1) That do not meet minimum security standards stated in the acquisition and procurement specifications.

(2) For which a C&A authorization has not been obtained from the appropriate DAA.

*f.* Commanders are responsible for ensuring that ISS under their purview are operated in a manner consistent with the system C&A package and this regulation.

cryptography, and the assurance properties as specified in NSA-endorsed medium robustness protection profiles or the Protection Profile Consistency Guidance for medium robustness.

(3) *Basic robustness.* Basic robustness is the security services and mechanisms that equate to best commercial practices. Basic robustness technical solutions require, at a minimum, authenticated access control, NIST-approved key management algorithms, NIST FIPS-validated cryptography, and the assurance properties specified in NSA-endorsed basic robustness protection profiles or the Protection Profile Consistency Guidance for Basic Robustness.

*d. Level of total system exposure.* The appropriate level of protection for each functional security requirement will be determined using a combination of the mission assurance category, level of confidentiality, and level of robustness.

(1) Each IS will be reviewed against the mission assurance category definitions provided in DODI 8500.2, Enclosure 2, and assigned to a mission assurance category.

(2) Each IS will be assigned a confidentiality level based on the classification or sensitivity of the information processed, stored, or transmitted.

(3) Determine the applicable IA controls from DODI 8500.2.

(4) The identified controls for the level of total system exposure serve as the baseline IA requirements for C&A or reaccreditation and will be reassessed and revalidated every 3 years as a minimum.

#### **4-5. Minimum information assurance requirements**

All required risk analyses will evaluate and identify possible vulnerabilities and adverse security effects on associated ISs and networks. Although manual procedures are acceptable when an automated safeguard is not feasible, IA personnel will embed automated security safeguards into the design and acquisition of ISs to ensure a secure infrastructure.

*a. Prohibited activities.* In addition to the prohibited activities listed in AR 25-1, the following activities are specifically prohibited by any authorized user on a Government provided IS or connection:

(1) Use of ISs for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes.

(2) Installation of software, configuration of an IS, or connecting any ISs to a distributed computer environment (DCE), for example the SETI project or the human genome research programs.

(3) Modification of the IS or software, use of it in any manner other than its intended purpose, or adding user-configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications. These applications create exploitable vulnerabilities and circumvent normal means of securing and monitoring network activity and provide a vector for the introduction of malicious code, remote access, network intrusions or the exfiltration of protected data.

(4) Attempts to strain, test, circumvent, or bypass network or IS security mechanisms, or to perform network or keystroke monitoring. RCERTs, Red Team, or other official activities, operating in their official capacities only, may be exempted from this requirement.

(5) Physical relocation or changes to configuration or network connectivity of IS equipment.

(6) Installation of non-Government-owned computing systems or devices without prior authorization of the appointed DAA including but not limited to USB devices, external media, personal or contractor-owned laptops, and MCDs.

(7) Release, disclose, transfer, possess, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

(8) Sharing personal accounts and authenticators (passwords or PINs) or permitting the use of remote access capabilities through Government provided resources with any unauthorized individual.

(9) Disabling or removing security or protective software and other mechanisms and their associated logs from IS.

*b. Accreditation.* ISs and networks will be accredited in accordance with interim DOD and Army DIACAP documentation and Army supplemental worthiness guidance.

*c. Access control.* IA personnel will implement system and device access controls using the principle of least privilege (POLP) via automated or manual means to actively protect the IS from compromise, unauthorized use or access, and manipulation. IA personnel will immediately report unauthorized accesses or attempts to their servicing RCERT in accordance with Section VIII, Incident and Intrusion reporting. Commanders and DAAs will—

(1) Enforce users' suspensions and revocation for violations of access authorization or violation in accordance with para 3-3c(13).

(2) Develop the approval processes for specific groups and users.

(3) Validate individual security investigation (or approve interim access) requirements before authorizing IS access by any user.

(4) Verify systems are configured to automatically generate an auditable record or log entry for each access granted or attempted.

(5) Validate that systems identify users through the user's use of unique user identifications (USERIDs).  
(6) Validate that systems authenticate users through the use of the CAC as a two-factor authentication mechanism. The CAC has certificates on the integrated circuit chip (ICC), and will be used as the primary user identifier and access authenticator to systems.

(7) Validate system configurations to authenticate user access to all systems with a minimum of a USERID and an authenticator when the systems are incapable of CAC enablement until these are replaced. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password.

(8) Verify that system configurations use password-protected screen savers, screen locks, or other lockout features to protect against unauthorized access of ISs during periods of temporary non-use. Ensure such mechanisms automatically activate when a terminal is left unattended or unused. The DOD activation standard is established at 15 minutes. Establish a shorter period when IS are used in a multinational or coalition work area. In instances where the unattended lockout feature hinders operations, for example; standalone briefing presentation systems, medical triage devices, or operating room systems status; the DAA and SO can approve longer timeouts as an exception only when it imposes a minimum of risk, other control mechanisms are enabled to mitigate these risks, and documented in the C&A package. However the timeout feature will never be disabled and the system will never remain unattended during this extended use period. Exceptions will never be granted for matters of convenience or ease of use.

(9) Validate that system configurations prohibit anonymous accesses or accounts (for example, Student1, Student2, Patron1, Patron2, anonymous).

(10) Prohibit the use of generic group accounts. Permit exceptions only on a case-by-case basis when supporting an operational or administrative requirement such as watch-standing or helpdesk accounts, or that require continuity of operations, functions, or capabilities. IAMs will implement procedures to identify and audit users of group accounts through other operational mechanisms such as duty logs.

(11) Verify that system configurations limit the number of user failed log-on attempts to three before denying access to (locking) that account, when account locking is supported by the IS or device. If IS-supported, the system will prevent rapid retries when an authenticator is incorrectly entered and gives no indications or error messages that either the authenticator or ID was incorrectly entered (for example, implement time delays between failed attempts).

(12) Verify that system configurations generate audit logs, and investigate security event violations when the maximum number of authentication attempts is exceeded, the maximum number of attempts from one IS is exceeded, or the maximum number of failed attempts over a set period is exceeded.

(13) Reinstate accesses only after the appropriate IA (for example, SA/NA) personnel have verified the reason for failed log-on attempts and have confirmed the access-holder's identity. Permit automatic account unlocking, for example, after an established time period has elapsed, as documented in the C&A package and approved by the DAA, based on sensitivity of the data or access requirements.

(14) If documented in the C&A package and authorized by the DAA, time-based lockouts (that is, access is restricted based on time or access controls based on IP address, terminal port, or combinations of these) and barriers that require some time to elapse to enable bypassing may be used. In those instances the DAA will specify, as a compensatory measure, the following policies:

- (a) Implement mandatory audit trails to record all successful and unsuccessful log-on attempts.
  - (b) Within 72 hours of any failed log-on and user lockout, IA personnel will verify the reason for failure and implement corrective actions or report the attempted unauthorized access.
  - (c) The SA will maintain a written record of all reasons for failure for 1 year.
- (15) Enforce temporary disabling of all accounts for deployed forces on garrison networks unless the accounts are operationally required.

(16) Create and enforce procedures for suspending, changing, or deleting accounts and access privileges for deployed forces in the event of capture, loss, or death of personnel having network privilege-level access.

(17) Create and enforce access auditing, and protect physical access control events (for example, card reader accesses) and audit event logs for physical security violations or access controls to support investigative efforts as required.

*d. Remote access (RA).*

(1) Systems being used for remote access must meet security configurations to include IAVM, certification and accreditation standards, and will employ host-based security, for example a firewall and IDS, with AV software before authorization to connect to any remote access server. Security configurations will be reviewed quarterly.

(2) Encrypt log-in credentials as they traverse the network as required for the level of information being accessed or required for need-to-know separation.

(3) Encrypt all RA for network configuration or management activities regardless of classification level, device, or access method.

(4) Users will protect RA ISs and data consistent with the level of information retrieved during the session.

(5) Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.

(6) Remote access users will read and sign security and end-user agreements for remote access annually as a condition for continued access.

*e. Remote access servers (RASs).*

(1) Secure remote terminal devices consistent with the mode of operation and sensitivity of the information and implement non-repudiation measures when necessary.

(2) Any IS that provides RAS capabilities will employ host-based firewalls and intrusion detection systems to detect unauthorized access and to prevent exploitation of network services.

(3) Any RAS being accessed remotely will employ a "Time-Out" protection feature that automatically disconnects the remote device after a predetermined period of inactivity has elapsed, dependent on classification level of the information, but no longer than 10 minutes.

(4) Remote access users will be required to authenticate all dial-in operations with a unique USERID and password, compliant with the remote authentication dial-in user system (RADIUS) standard.

(5) All RAs will terminate at a centrally managed access point located within a demilitarized zone (DMZ) that is configured to log user activities during a session.

(6) Prohibit all RA (that is, virtual private network (VPN), dial-in) to individual ISs within an enclave (that is, behind the DMZ firewall).

(7) DOIMs and IAMs must ensure all remote access servers (RASs) undergo CM and C&A processes.

(8) Stand alone dial-back modems and modem systems that authenticate using RADIUS are the only allowable dial-in modems.

(9) Physical security for the terminal will meet the requirements for storage of data at the highest classification level received at the terminal and must be implemented within a restricted access area.

(10) Data between the client and the RAS will be encrypted to provide confidentiality, identification, non-repudiation and authentication of the data. The CAC provides the user with an official certificate.

(11) Approved telework or telecommuting access will be in accordance with established DOIM, RCIO, and NETCOM/9th SC (A) C&A access procedures from a Government provided system only. Ad hoc telework access (defined as one-time, informal, or on an infrequent basis) will be through existing and approved external access methods or portals such as Terminal Server Access Control System (TSACS) or the Army Knowledge Online (AKO) Web site.

(12) Outside the continental United States (OCONUS) telework procedures and authorization will be approved by the DAA and RCIO on a case-by-case basis and documented in the C&A package.

(13) Audit all RAS connections at a minimum weekly.

(14) Review RAS devices biweekly for security configuration, patches, updates, and IAVM compliance.

*f. Configuration management requirements.* The following policy will be the minimum used for the CM of all systems:

(1) All CM plans will include a maintenance and update strategy to proactively manage all IS and networks with the latest security or application updates. While IAVM is part of a CM strategy, it is not all-inclusive for every IS in use in the Army. All ISs will have a vulnerability management strategy for testing and maintaining patches, updates, and upgrades.

(2) Hardware and software changes to an accredited IS, with an established baseline, will be effected through the CM process.

(3) The CCB or the CMB for a site must approve modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any system or network without the express written consent of the IAM and the CMB or CCB. In the absence of a CCB or CMB, the appropriate commander or manager will provide the consent on the advice of the cognizant IA official.

(4) Modifying, installing, or downloading of any software on any computer system may affect system C&A and must be evaluated and approved by the IAM with the local CMB, CCB, and DAA.

(5) Configuration management controls, including version controls, will be maintained on all software development efforts; RDT&E activities; follow-on test and evaluation (FOT&E) activities; and other related tests by the software designer. A CM "baseline image" will be created, documented, kept current, and maintained by network and system administration personnel for all ISs within their span of control. Exceptions to this baseline image will be documented in the C&A package and approved by the DAA.

(6) The minimum baseline configuration for ISs will be the published Security Technical Implementation Guide (STIG) requirements or the common criteria protection profiles for IA products, as available or supplemented and published by DOD and NETCOM/9th SC (A), with any changes documented. STIGs are located at: <http://iase.disa.mil/stigs/index.html>.

(7) Prohibit default installations of "out of the box" configurations of COTS purchased products. COTS purchased products will require system CM and IAVM compliance as a minimum. Comprehensive vulnerability assessments of

the test IS will be conducted and documented before and after installation of any COTS products under consideration for CM review or approval.

(8) Upon acceptance for operational use (whether developmental, GOTS, or COTS), keep software under close and continuous CM controls to prevent unauthorized changes.

(9) ISs must meet minimum levels of total system exposure. See paragraph 4-4 and DODI 8500.2 to establish IA baseline requirements.

*g. Assessments.* Commanders will verify that IA personnel conduct initial and continual assessments to detect IS and network vulnerabilities using approved tools, tactics, and techniques to facilitate the risk management process and to ensure compliance with network management, CM, IAVM requirements, and security policies and procedures. Commanders and IA personnel will ensure that all networks and networked ISs undergo a self-assessed, vulnerability assessment scan quarterly. Prohibit the use of commercial scanning services or vendors without the CIO/G6's chief information security officer's (CISO) approval.

*h. Auditing.* SAs will configure ISs to automatically log all access attempts. Audits of IS will be either automated or manual means. SAs will implement audit mechanisms for those ISs that support multiple users.

(1) Use audit servers to consolidate system audit logs for centralized review to remove the potential for unauthorized editing or deletion of audit logs in the event of an incident or compromise.

(2) Commands, organizations, tenants, activities, and installations will support centralized audit server implementations in the enterprise.

(3) Centralized audit servers logs will be maintained for a minimum of 1 year.

(4) Conduct self-inspections by the respective SA/NA or IA manager.

(5) Enable and refine default IS logging capabilities to identify abnormal or potentially suspicious local or network activity—

*(a)* Investigate all failed login attempts or account lockouts.

*(b)* Maintain audit trails in sufficient detail to reconstruct events in determining the causes of compromise and magnitude of damage should a malfunction or a security violation occurs. Maintain system audit logs locally for no less than 90 days.

*(c)* Retain classified and sensitive IS audit files for 1 year (5 years for SCI systems, depending on storage capability).

*(d)* Provide audit logs to the ACERT, Army-Global Network Operations and Security Center (A-GNOSC), IE, or CI personnel to support forensic, criminal, or counter-intelligence investigations as required.

*(e)* Review logs and audit trails at a minimum weekly, more frequently if required, and take appropriate actions.

*i. Contingency planning.* A contingency plan is a plan for emergency response, backup operations, transfer of operations, and post-disaster recovery procedures maintained by an activity as a part of its IA security program. Commanders will create and practice contingency plans for each IS (a single IS or local area network (LAN)) for critical assets as identified by the data owner or commander to support continuity of operations planning (COOP). See DA Pam 25-1-2 for additional guidance and procedures for developing contingency plans. Exercise contingency plans annually.

*j. Data integrity.*

(1) Implement safeguards to detect and minimize unauthorized access and inadvertent, malicious, or non-malicious modification or destruction of data.

(2) Implement safeguards to ensure that security classification levels remain with the transmitted data.

(3) DAA will identify data owners for each database on their networks. Only the original classification authority (OCA) is authorized to change the data classification.

(4) DAA will develop and enforce policies and procedures to routinely or automatically backup, verify, and restore (as required) data, ISs, or devices at every level. These policies and procedures will be captured in the C&A package.

(5) Use data or data sources that have verifiable or trusted information. Examples of trusted sources include, but are not limited to, information published on DOD and Army sites and vendor sites that use verified source code or cryptographic hash values.

(6) Protect data at rest (for example, databases, files) to the classification level of the information with authorized encryption and strict access control measures implemented.

*k. C&A package.* The C&A package will be available to the site-assigned IASO for the life of each IS or LAN, including operational, prototype, test, or developmental systems. This C&A package will include at a minimum the System Identification Profile (SIP), Scorecard, and plan of action and milestones (POA&M).

*l. IA product acquisition.* All security-related COTS hardware, firmware, and software components (excluding cryptographic modules) required to protect ISs will be acquired in accordance with public law and will have been evaluated and validated in accordance with appropriate criteria, schemes, or protection profiles (<http://www.niap-nist.gov/>) and this regulation. IA products listed on the IA Approved Products List (APL) available on the IA website, will be evaluated/selected first, and then procured through Army Computer Hardware, Enterprise, Software and Solutions contract vehicles before other IA products are procured. For PEO/PM's, the CSLA BPA requirements

only applies to the procurement of COMSEC devices. All GOTS products will be evaluated by NSA or in accordance with NSA-approved processes. NETCOM/9th SC (A) and CIO/G-6 may approve exceptions to IA products evaluations when no criteria, protection profile, or schema exists or is under development, and the removal or prohibition of such an IA product would significantly degrade or reduce the ability of personnel to secure, manage, and protect the infrastructure.

*m. Notice and consent procedures.* Commanders will verify that all computers under their control, independently, prominently and completely display the Notice and Consent Banner immediately upon users' authentication to the system, including, but not limited to, web, ftp, telnet, or other services access.

(1) General Notification: Army users of DOD telecommunications systems or devices are advised that DOD provides such systems and devices for conducting authorized use. Users are subject to telecommunications monitoring, including their personal communications and stored information.

(2) Using Government telecommunications systems and devices constitutes the user's consent to monitoring.

(3) Users will be advised that there is no expectation of privacy while using ISs or accessing Army resources.

(4) The user must take a positive action to accept the terms of the notice and consent warning banner before a successful logon is completed.

(5) Post appropriate warning banners and labels in accordance with this regulation.

(6) The following access warning banner replaces the warning banner in AR 380-53 and will not be modified further. The banner to be posted on Army networks, systems, and devices will state—

(7) "YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY." By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

(8) For those personal computing devices such as Blackberries and other PDAs that have technical limitations to the full banner, then the only approved solution will be: "I've read & consent to terms in IS user agreement."

(9) For media devices, services, protocols, and other limited text input requirements other than PDA devices requiring access, such as routers, firewalls, bannered access ports, and so forth. This banner will be "Subject to Army Warning banner in AR 25-2, 4-5m(7)."

*n. Virus protection.* Implement the virus protection guidance provided below on all ISs and networks, regardless of classification or purpose—

(1) Users and SAs will scan all files, removable media, and software, including new "shrink-wrapped" COTS software, with an installed and authorized AV product before introducing them onto an IS or network. Files, media and software found to be infected with a virus will be reported by users to the SA.

(2) To minimize the risks of viruses, implement the following countermeasures:

(a) SAs will configure all ISs with a current and supportable version of the AV software configured to provide real-time protection from the approved products list with automated updates and reporting enabled.

(b) IA personnel should take the multilevel approach to virus detection by installing one AV package on the workstations and a different AV package on the servers.

(c) SAs will update virus definitions at a minimum weekly, or as directed by the ACERT for immediate threat reduction. Virus definition availability is based on vendors' capabilities. IA personnel will institute automated antivirus definition updates as published or available from authorized DOD or Army sites.

(3) IA personnel will train users to recognize and report virus symptoms immediately.

(4) IAMS will implement virus-reporting procedures to support DOD and Army reporting requirements.

*o. Mobile code.*

(1) Mobile code is executable software, transferred across a network, downloaded, and executed on a local system without notification to, or explicit installation and execution by, the recipient.

(2) Mobile code has the potential to severely degrade operations if improperly used or controlled. The objective of the mobile code security policy is to deny untrusted mobile code the ability to traverse the Army enterprise. As a minimum, the Army mobile code mitigation policy will be implemented to support the DOD mobile code policy. Untrusted mobile code will not be allowed to traverse the enterprise unless NETCOM/9th SC (A) CCB-approved mitigating actions have been emplaced.

*p. Layering.*



(1) Layering is a process of implementing similar security configurations or mechanisms at multiple points in an IS architecture. Doing so eliminates single points of failure, provides redundant capabilities, increases access granularity and auditing, and implements an effective computer or network attack detection and reaction capability.

(2) The Army enterprise IA security DiD structure requires a layering of security policies, procedures, and technology, including best practices such as redundant capabilities or use of alternative operating systems, to protect all network resources within the enterprise. Layered defenses at the boundaries, for example, include, but are not limited to using inbound and outbound proxy services, firewalls, IDSs, IPSs, and DMZs.

*q. Filtering.* Filtering policies will block ingress and egress services, content, sources, destinations, ports, and protocols not required or authorized across the enterprise boundary. Router and firewall access control lists (ACLs) provide a basic level of access control over network connections based on security or operational policy.

(1) Filtering at the enterprise boundary is the primary responsibility of the NETCOM/9th SC (A) TNOSCs using tools and techniques applied at the enterprise level.

(2) At all levels subordinate to NETCOM/9th SC (A), filtering policies and technology will be implemented and layered throughout the architecture and enforced at all capable devices. Audit and system or device generated event logs will be provided to NETCOM/9th SC (A). These policies should be complementary.

(3) Filtering products and techniques are intended to proactively reduce ingress and egress security threats to enterprise systems and information without targeting specific individuals. The most common threats are associated with malicious content, misuse, security policy violations, content policy violations, or criminal activity. Threat mitigation policies will be incorporated, configured, and monitored to reduce or identify these threats and include, but are not limited to, ACL configuration on routing devices to prevent access to unauthorized sites, AV installations, cache or proxy servers (to maintain connection state), firewalls, mail exchange configurations (for example, auto-deletion of attachments), network monitoring software such as IDS or Intrusion Prevention System (IPS) configured to terminate suspicious traffic, content management, or web filtering applications.

*r. AUP.*

(1) Commanders and Directors will implement an AUP for all user accesses under their control (see the sample AUP at appendix B).

(2) Users will review and sign an AUP prior to or upon account activation. Digital signatures are authorized.

(3) IA personnel will maintain documented training records.

(4) DOD policy states that Federal Government communication systems and equipment (including Government-owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only.

(5) Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Official use can also include other use authorized by a theater commander for Soldiers and civilian employees deployed for extended periods away from home on official business.

(6) Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes can also include limited personal use established by appropriate authorities under the guidelines of the Joint Ethics Regulation (DOD 5500.7-R).

(7) Certain activities are never authorized on Army networks. AUPs will include the following minimums as prohibited. These activities include any personal use of Government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

*s. Monitoring networks.*

(1) Network monitoring includes any of a number of actions by IA personnel aimed at ensuring proper performance and management. When any of these monitoring activities involve intercepting (capturing in real time) the contents of wire or electronic communications, they must fall within the limits of the service provider exception to the Federal wiretap statute. The service provider exception allows system and network administrators to intercept, use, and disclose intercepted communications as long as the actions are conducted in the normal course of employment and the SA/NA is engaged in an activity that is necessary to keep the service operational or to protect the rights or property of the service provider. Therefore, IA personnel must consult with legal counsel to ensure that their activities involving systems management and protection are properly authorized.

(2) IA personnel performing ingress and egress network monitoring or filtering activities are authorized to use CIO/G-6-approved automated monitoring tools maintained and configured by NETCOM/9th SC (A) as network devices to aid in the performance and management. It is important to recognize that the SA/NA does not have unlimited authority in the use of these network monitoring tools. The approved tool may contain technical capabilities beyond those tasks for which the tool was approved; as such the IA personnel must ensure that approved tools are used only for their intended purpose.

(3) **IA personnel will not use unapproved IA tools, use IA tools for unapproved purposes, or misuse automated IA tools.** Violations will be reported through appropriate command channels to the CIO/G-6. Exceptions to the configuration of these devices will be approved on a case-by-case basis by NETCOM/9th SC (A).

(4) In general terms, IA personnel and SAs/NAs do not engage in blanket network monitoring of internal communications. However, the Army reserves the right at any time to monitor, access, retrieve, read, or disclose internal communications when a legitimate need exists that cannot be satisfied by other means pursuant to para 4-5r, below.

(5) As a matter of normal auditing, SAs/NAs may review web sites logs, files downloaded, ingress and egress services and similar audited or related information exchanged over connected systems. Supervisors and managers may receive reports detailing the usage of these and other internal information systems, and are responsible for determining that such usage is both reasonable and authorized.

(6) As a matter of normal auditing, SAs/NAs may store all files and messages through routine back ups to tape, disk, or other storage media. This means that information stored or processed, even if a user has specifically deleted it, is often recoverable and may be examined at a later date by SAs/NAs and others permitted by lawful authority.

(7) SAs/NAs may provide assistance to Army supervisory and management personnel, under lawful authority, to examine archived electronic mail, personal computer file directories, hard disk drive files, and other information stored on ISs. This information may include personal data. Such examinations are typically performed to assure compliance with internal policies; support the performance of administrative investigations; and assist in the management and security of data and ISs.

(8) When IA personnel discover information during the course of their normal activity that indicates a violation of acceptable use or a possible criminal offense, they will immediately report the finding to their Commander. The commander will immediately report known or suspected criminal activity to LE and will consult with legal counsel concerning activities that appear merely to violate acceptable use. IA personnel will retain and provide information related to the matter to LE when required.

(9) **With the exceptions of the SA/NA as identified below, Army personnel and contractors are prohibited from browsing or accessing other user's e-mail accounts.**

(10) The SA/NA may only intercept, retrieve, or otherwise recover an e-mail message and any attachments thereto, only under the following circumstances:

(a) With consent (expressed or implied) of a party to the communication involved.

(b) In response to a request for technical assistance from:

1. LE/CI personnel pursuant to a properly authorized LE/CI investigation.

2. A supervisor as part of a non-investigatory management search in accordance with paragraph 4-5r, below.

3. An investigating officer pursuant to a properly authorized administrative investigation (for example, a preliminary inquiry under Rule for Courts-Martial 303, an informal investigation under AR 15-6, or a preliminary inquiry under AR 380-5).

4. Information systems security monitoring personnel pursuant to properly authorized IS security monitoring activities.

5. Inspector General personnel pursuant to an authorized inspection, investigation, or inquiry.

(11) The SA/NA may remove any e-mail, file, or attachment that is interfering with the operation of an IS without consent of the originator or recipient. The SA/NA will notify the originator and recipient of such actions.

(12) The SA/NA is not authorized to use techniques or software to penetrate or bypass user's information protections (for example, content restrictions or read-only protections used to maintain or enforce document integrity, version control, or need-to-know enforcement).

*1. Management search.* In the absence of the user (for example, TDY, extended hospital stay, incapacitation, emergency operational requirement), only the SA/NA is authorized limited access to the user's files to support administrative management searches to provide the requested information as required for official purposes. When such access is requested, the SA will—

(1) Brief the supervisor as to the limits of accessing the user's data files.

(2) Limit the scope of the authorized search to those files reasonably related to the objective of the search (that is, e-mail access would not be reasonable when searching for a word document file).

(3) Limit the search to the time necessary to locate the required data in the most relevant file location.

(4) Inform the individual of requested file access as soon as possible after such requests, and document this access in a memorandum.

(5) SAs/NAs will not grant unrestricted supervisory access to individual information, data files, or accounts.

(6) SAs/NAs will not access individual information or data files unless conducting a management search, an authorized administrative search, or supporting a LE/CI authorized investigation.

(7) SAs/NAs may conduct an authorized investigative or management search of assigned IS upon an individual's termination of employment, death, or other permanent departure from the organization to retrieve data and files associated with the organizational mission.



3. Identification requirements when dealing with others through oral, written, and electronic communications, such as e-mail.

4. Department of the Army employees or contractors who are FNs and are direct or indirect hires, currently appointed in IA positions, may continue in these positions provided they satisfy the provisions of paragraph 4-14, DODD 8500.1, DODI 8500.2, and DOD 5200.2-R; are under the supervision of an IAM who is a U.S. citizen; and are approved in writing by the DAA and captured in the C&A package.

5. FNs assigned into IT positions will be subject to the same (or equivalent) vetting as U.S. citizens.

6. FNs may hold or be authorized access to IT-II and IT-III positions provided the required background investigation has been completed or favorably adjudicated.

7. Additionally, an FN may be assigned to an IT-I position only after the DAA who owns the system and the data owner who owns the information sign a waiver and the assignment has been approved by the CIO/G-6. The approvals will become part of the C&A package. Sign and place the waiver in the individual's security file before requesting the required background investigation. The required background investigation must be completed and favorably adjudicated before authorizing IT-I access to DA systems/networks.

8. Do not assign FNs to IT-I, IT-II, or IT-III positions on an interim basis before a favorable adjudication of the required personnel security investigation.

i. Generally, an FN or official representative is not authorized access to the U.S. controlled SIPRNET terminal workspace. If an authorized foreign official or national working at a U.S. Army site has a requirement for accessing the SIPRNET, the commander will submit an exception to policy through the DAA to the RCIO IAPM, to be forwarded to the HQDA CIO/G-6, and reviewed by the DCS, G-2 Foreign Disclosure Directorate prior to disposition. CIO/G-6 will coordinate the request with the Army staff and forward to DISA. These requests will be staffed with the presumption of denial. Apply the procedures of this section after DISA's approval and any additional guidance provided by DISA on the connection process for FNs. E-mail signature blocks will be automatically generated for all FNs, and include the foreign individual's nationality and position. The approvals will become part of the C&A package.

## **Section VI**

### **Information Systems Media**

#### **4-16. Protection requirements**

a. All IS equipment and facilities used for processing, handling, and storing classified data will be operated and secured where applicable per the DCID 6/3, AR 380-5, this regulation, or Joint DODIIS Cryptologic SCI Information Systems Security Standards (JDCSISSS).

b. All Army personnel and contractors will mark, ship, store, process, and transmit classified or sensitive information in accordance with AR 380-5.

c. Control ISs containing non-removable, non-volatile media used for processing classified information.

d. Commanders, Directors, and IA personnel will verify procedures and train users, administrators and security personnel in processes for spillage incidents of higher-level or classified information to a lower-level IS.

e. SAs will configure ISs to apply security or handling markings automatically when possible or available.

f. SAs will configure ISs to display the classification level on the desktop or login screen (for example, wallpaper, splash screen) when the device is locked, the user is logged off, or the IS is used in spanning multi-classification networks through the use of a KVM device.

g. All Army personnel and contractors will not transmit classified information over any communication system unless using approved security procedures and practices including, encryption, secure networks, secure workstations, and ISs accredited at the appropriate classification level.

#### **4-17. Labeling, marking, and controlling media**

a. Unless write-protected or read-only, all personnel will protect and classify media inserted into a system at the highest level the system is accredited to process until the data or media is reviewed and downgraded by the IASO.

b. All personnel will clear removable media before reusing in ISs operating at the same or higher protection level.

c. All personnel will mark and control all media devices, peripherals, and ISs as follows:

(1) TS or SCI or intelligence data per DCID 6/3, DCID 1/7 and JDCSISSS as applicable.

(2) Classified media per AR 380-5 requirements.

(3) FOUO media per AR 25-55 requirements.

(4) Privacy Act media per AR 340-21 requirements.

(5) NATO information per AR 380-5 requirements.

d. All personnel will mark and control the media or IS after determination of the classification level of the data placed on the media. Implement media accountability procedures based on the type of media and the classification of the data as required above.

---

### Acceptable Use Policy

**1. Understanding.** I understand that I have the primary responsibility to safeguard the information contained in *classified network name (CNN)* and/or *unclassified network name (UNN)* from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use.

**2. Access.** Access to *this/these network(s)* is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy.

**3. Revocability.** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing.

**4. Classified information processing.** CNN is the primary classified IS for *(insert your organization)*. CNN is a US-only system and approved to process *(insert classification)* collateral information as well as: *(insert additional caveats or handling instructions)*. CNN is not authorized to process *(insert classification or additional caveats or special handling instructions)*.

a. CNN provides communication to external DoD *(or specify other appropriate U.S. Government)* organizations using the SIPRNET. Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telnet (insert others as appropriate)*.

b. The CNN is authorized for *SECRET* or lower-level processing in accordance with *accreditation package number, identification, etc.*

c. The classification boundary between CNN and UNN requires vigilance and attention by all users. CNN is also a US-only system and not accredited for transmission of NATO material.

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the CNN is a security violation and will be investigated and handled as a security violation or as a criminal offense.

**5. Unclassified Information Processing.** UNN is the primary unclassified automated administration tool for the *(insert your organization)*. UNN is a US-only system.

a. UNN provides unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and internet networking protocols such as *web, ftp, telnet (insert others as appropriate)*.

b. UNN is approved to process UNCLASSIFIED, SENSITIVE information in accordance with *(insert local regulation dealing with automated information system security management program)*.

c. The UNN and the Internet, as viewed by the *(insert your organization)*, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the SIPRNET and Internet.

---

Figure B-1. Acceptable use policy

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Government Motion  
to Take Judicial Notice

Enclosure 2

3 August 2012

Security

# **Department of the Army Information Security Program**

Headquarters  
Department of the Army  
Washington, DC  
29 September 2000

**UNCLASSIFIED**

have confidence in the sharing of information with other agencies, the national, DOD, and DA policy, contained in this regulation, will be followed.

b. Unless otherwise noted, requests for waivers to the requirements contained in this regulation, will be submitted, through command channels, to DAMI-CH. Waivers to DOD requirements will be forwarded by DAMI-CH, for decision to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). For requirements related to Two-Person Integrity (TPI), RD, Foreign Government Information (FGI) (including North Atlantic Treaty Organization (NATO)), and security arrangements for international programs, waivers will be forwarded to the Under Secretary of Defense (Policy)(USD(P)). Waivers for SAPs will be submitted, through SAPs channels, to DAMI-CH for coordination with TMO and, as required, forwarded to the Under Secretary of Defense (Special Programs) (USD(SP)). The ASD(C3I) and USD(P) are responsible for notifying the Director of the ISOO of the waivers approved that involve EO 12958 and its implementing directives.

c. Before submitting a request for waiver, the requesting authority will consider risk management factors such as criticality, sensitivity, and value of the information, analysis of the threats both known and anticipated, vulnerability to exploitation, and countermeasure benefits versus cost (national security cost and resource cost). Requests for waiver must contain sufficient information to permit a complete and thorough analysis to be made of the impact on national security if the waiver is approved. The waiver request will also describe all the factors creating the special situation and the alternative or compensatory measures which make sure the protection afforded the information is sufficient to reasonably deter and detect loss or unauthorized disclosure. The requesting command will maintain documentation regarding approved waivers, including the alternative or compensatory measures approved and in use, and furnish this documentation, upon request, to other agencies and to other Army commands, with whom classified information or secure facilities are shared.

Note: Waivers granted before the effective date of this regulation are canceled no later than one year after the effective date of this regulation. New/updated waiver requests may be submitted prior to cancellation date.

d. Throughout this regulation there are references to policy subject to MACOM approval or subject to policy as the MACOM directs. Where that language, in substance, is used, the MACOM commander, or the HQDA SAAA, for cases involving HQDA and its Field Operating Agencies (FOA), can delegate such approval authority. The delegations will be in writing. A copy of such delegations will be maintained by the appointing official and reviewed periodically for review of need for continuation. Where this regulation specifically specifies waiver authority to a MACOM commander or the HQDA SAAA, that authority resides solely with the MACOM commander or HQDA SAAA and will not be further delegated.

## **Section VII**

### **Corrective Actions and Sanctions**

#### **1-20. General**

Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

#### **1-21. Sanctions**

a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—

- (1) Disclose classified or sensitive information to unauthorized persons.
- (2) Classify or continue the classification of information in violation of this regulation.
- (3) Violate any other provision of this regulation.

b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice (UCMJ) for violations of that Code and under applicable criminal law, if warranted.

c. Original classification authority will be withdrawn for individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

#### **1-22. Reporting of Incidents**

EO 12958, paragraph 5.7(e)(2), requires that the director of the ISOO be advised of instances in which classified information is knowingly, willfully, or negligently disclosed to unauthorized persons, or instances of classifying, or continuing the classification of, information in violation of this regulation. Reports of those instances will be submitted through command channels to DAMI-CH for forwarding to the director of the ISOO and other defense officials as appropriate. See chapter 10 for reporting of other security incidents.

## **Section VIII Reports**

### **1-23. Reporting Requirements**

HQDA is required to report data necessary to support various requirements of EO 12958. Commanders will respond to those data calls when so notified. MACOMs and the HQDA SAAA will also submit a consolidated annual report, for all units under their security responsibility, on SF 311, to reach DAMI-CH no later than 1 October, or other date specified by DAMI-CH, each fiscal year. The report will cover the preceding fiscal year. DAMI-CH will consolidate and submit the annual SF 311 report for the Army. Interagency Report Control Number 0230-GSA-AN applies to this report.

### **1-24. Command security inspections**

MACOM, agency, and MSC commanders will establish and maintain a self-inspection program for their command, and a program to inspect their subordinate units. The program must be based upon program needs and the degree of involvement with classified and sensitive information. The purpose of the program will be to evaluate and assess the effectiveness of the command's protection of classified and sensitive information and adherence to Army policy contained in this regulation. Inspections will be conducted annually unless the command's higher headquarters determines that the quantity of classified and sensitive holdings and material generated does not warrant that frequency. In those cases, inspections will occur not less frequently than once every other year. This will not dismiss other annual requirements outlined in this regulation.

## **Chapter 2 Classification**

### **Section I Classification Principles**

#### **2-1. Original vs. derivative classification**

a. Original classification is the decision to designate a certain item of information as classified, at a particular level, and for a certain duration of time. Often these decisions are communicated in a published Security Classification Guide (SCG). These decisions can only be made by persons designated in writing by either the SECARMY or the DCSINT as Original Classification Authorities (OCA). There are relatively few officials in the Army that have the authority to apply original classification, and relatively few instances of original classification, in most Army commands. Derivative classification is the incorporating, restating, paraphrasing, or generating in new form, information that has already been determined to be classified, and ensuring that it is classified and handled at the level that the OCA has already determined will be done. Derivative classification can be accomplished by any properly cleared personnel. Derivative classifiers are not required to be appointed or designated unless so directed by Command option. Most DA personnel that classify information do so in a derivative manner from some other document or source. Derivative classification is most commonly accomplished by marking classified material based on the guidance from an SCG or from the source document. The derivative classifier must have enough subject matter knowledge to properly interpret and apply the instruction of the classification guidance. The original classification authority decides what portion(s) of a plan, program, or project needs to be classified. The derivative classifier applies that decision to the same type of information restated or generated in a new form.

b. For example, an OCA could make the decision that the maximum effective range of Missile XYZ is classified. The classification authority issues a security classification guide that states that the maximum effective range of the missile will be classified at the SECRET level. When the missile is tested and the results are documented, the person who writes the report, states that the maximum effective range of Missile XYZ is 250 miles, derivatively classifying that item of information as SECRET. In this case, the classification is derived from the security classification guide. Most classification in the Department of the Army is done in a derivative manner. Those DA officials authorized to apply original classification decisions are relatively few in number.

#### **2-2. Policy**

Original classification is the initial determination by an OCA that an item of information could be expected to cause damage to national security if subjected to unauthorized disclosure. Damage to the national security means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of the information, to include the sensitivity, value, and utility of that information. It includes military operations in support of national objectives when those operations involve information that meets the criteria of classification. This decision will be made only by persons specifically authorized in writing to do so, have received training in the exercise of this authority, and have program or program support responsibility or cognizance over the information. The decision to

originally classify must be made based on the requirements of this regulation. Delegations of original classification authority will be limited to the minimum required and only to officials who have a demonstrable and continuing need to exercise it.

### **2-3. Delegation of authority**

a. The Secretary of the Army has been granted original classification authority by the President of the United States. TOP SECRET OCA can be delegated only by the SECARMY. SECRET and CONFIDENTIAL original classification authority can only be delegated by the DCSINT or by the SECARMY. Delegation of authority includes information at that level and any lower level(s) of classification. This authority cannot be redelegated.

b. Requests for OCA will be submitted, through command channels, to DAMI CH. These requests will specify the position title for which the authority is requested and detailed justification for the request. Original classification authority is assigned to a position title and not to an individual person. In order to ensure that the number of OCAs is strictly limited, the request must address why another OCA, within that official's command or area, cannot assume this responsibility.

c. Requests for original classification authority will be granted only when:

- (1) Original classification is required during the normal course of operations;
- (2) Sufficient expertise and information is available to the prospective original classification authority to allow effective classification decision making;
- (3) The need for original classification cannot be handled by other existing OCAs; or
- (4) Referral of decisions to existing original classification authorities, at the command or at higher levels in the chain of command, is not practical.

### **2-4. Required Training**

Officials who have been delegated original classification authority will receive training, as required by chapter 9 of this regulation, before exercising this authority.

## **Section II**

### **Derivative Classification**

#### **2-5. Policy**

DA personnel who generate material which is to be derivatively classified are responsible for making sure that the classification is properly applied based on the original source material marking and local security classification guides. DA personnel who apply derivative classification should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all or part of the basis for classification. Certain information that would otherwise be unclassified, may require classification when combined or associated with other unclassified information. This is referred to as classified by compilation. However, a compilation of unclassified items of information is normally not classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants classification. Similarly, a higher classification may be assigned to compilations of information that warrants higher classification than that of its component parts. Classification on this basis shall be fully supported, in writing, accompanying the compilation document. See paragraph 2-8 for specific classifying criteria.

#### **2-6. Accuracy responsibilities**

Officials who sign or approve derivatively classified material are responsible for the accuracy of the derivative classification. This applies to all forms of material and information regardless of the media involved. Personnel accomplishing derivative classification will—

- a. Observe and respect the classification determinations made by original classification authorities.
- b. Apply markings or other means of identification to the derivatively classified material, as required by this regulation, at the level and for the duration specified by the classification guide or source document. Where classification instructions do not reflect the new marking requirements of EO 12958, mark the level of classification as directed by the classification guide or source document and follow this regulation for all other marking requirements. Derivative classifiers are encouraged to keep informal records of which portions of a draft document are classified and by which source to make the classification of the finished product easier.
- c. Use only authorized sources such as classification guides, other forms of official classification guidance, and markings on source material, from which the information is extracted. Refrain from guesswork.
- d. Use caution when paraphrasing or restating information extracted from a classified source to determine whether the classification could have been changed in the process.
- e. Take appropriate and reasonable steps to resolve doubt or conflicts in classification. In cases of apparent conflict between an SCG and a classified source document, concerning a discrete item of information, the instructions in the SCG will take precedence unless the source document is signed by the original classification authority. In such cases,

the OCA, or the point of contact for answering questions on classification, will be consulted. In the event that it is not possible to consult the OCA, the more restrictive classification instruction will be followed.

f. Make a list of sources used when material is derivatively classified based on "Multiple Sources" (more than one SCG, classified source document, or any combination). A copy of this list will be included in, or attached to, the file or record copy of the material. Derivative classifiers are encouraged to include this listing with all copies of the document, to make later declassification review easier if the file or record copy is unavailable.

g. Contact the classifier of the source document for resolution in cases in which the derivative classifier believes the classification applied to the information is not accurate.

## **Section III**

### **The Original Classification Process**

#### **2-7. General**

The decision to apply original classification requires the application of judgment, on the part of the classifier, that the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, and that the probable damage can be identified or described. It is not necessary for the original classifier to produce a written description of the damage at the time of classification, but the classifier must be prepared to do so if the information becomes the subject of a classification challenge, a request for mandatory review for declassification, or a request for release under the Freedom of Information Act. The decision to classify also has operational and resource impacts as well as impacts affecting the United States technological base and foreign relations. The decision to classify should consider all relevant factors. If there is doubt about classification, the OCA will research the matter to make an informed decision. If, after such research, there is a significant doubt about the need to classify information, it will not be classified. In making a decision to originally classify an item of information, an original classification authority will—

- a. Determine that the information has not already been classified.
- b. Determine that the information is eligible for classification pursuant to paragraph 2-8 of this regulation.
- c. Determine that classification of the information is a realistic course of action and that the information can be protected from unauthorized disclosure when classified.
- d. Decide that unauthorized disclosure could reasonably be expected to cause damage to the national security and that this disclosure is identifiable and can be described.
- e. Select the appropriate level or category of classification and/or sensitivity to be applied to the information, based on a judgement as to the degree of damage unauthorized disclosure could cause.
- f. Determine and include the appropriate declassification, downgrading, and/or exemption category instruction(s) to be applied to the information, when applicable.
- g. Make sure that the classification decision is properly communicated so that the information will receive appropriate protection. Security classification guides will be used in this regard where appropriate (see paragraph 2-16).

#### **2-8. Classification criteria**

U.S. classification can only be applied to information that is owned by, produced by or for, or is under the control of, the United States Government. This is determined by the original classification authority that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the information falls within one or more of the following categories specified in section 1.5 of EO 12958:

- a. Military plans, weapons systems, or operations.
- b. Foreign government information.
- c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
- d. Foreign relations or foreign activities of the United States, including confidential sources.
- e. Scientific, technological, or economic matters relating to the national security.
- f. United States Government programs for safeguarding nuclear materials or facilities.
- g. Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security. Note: When used, these seven classification categories are referred to by their reference letter, preceded by "1.5," the reference location within the EO. For example, "Military plans, weapons systems, or operations" would be "1.5(a)." See paragraph 4-9 for further details on "Classified by" marking.

#### **2-9. Possibility of Protection**

- a. The OCA must determine that, if classification is applied or reapplied, there is a reasonable possibility that the information will be provided protection from unauthorized disclosure.
- b. The reclassification of information which was once classified but was declassified and officially released to the public, by an authorized Army official, and had wide-spread access by the public, is prohibited. Army information that has not previously been disclosed to the public, under proper Army authority, can be classified or reclassified. This includes after a command has received a request for it. However, only if the reclassification is accomplished on a



document-by-document basis, with the participation, or under the direction of, the SECARMY, the Under Secretary of the Army, or the DCSINT. Guidance from DAMI-CH will be requested in those instances. The information that is reclassified must meet the criteria for classified information established in EO 12958 or successor orders and directives. In considering issues of reclassification or classification of previously unclassified information, the OCA will—

(1) Determine that control of the information has not been lost and can still be prevented from being lost; and  
(2) In the case of information released to secondary distribution centers, determine that no secondary distribution has been made and can still be prevented.

c. Classified information will not be declassified automatically as a result of any unauthorized disclosure of identical or similar information. In these cases, the OCA will review the situation to determine if continued classification is warranted. However, such disclosures require immediate determination of the degree of damage to the national security and reevaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted.

## **2-10. Levels of classification**

a. Once a decision is made to classify, information will be classified at one of the three levels listed below. For each level, the OCA must be able to identify or describe the damage that unauthorized disclosure reasonably could be expected to cause to the national security. These levels are:

(1) TOP SECRET – Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

(2) SECRET – Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

(3) CONFIDENTIAL – Will be applied to information in which the unauthorized disclosure could reasonably be expected to cause damage to the national security.

b. If there is doubt about the classification level, the OCA will research the matter to make an informed decision. If significant doubt still remains about the classification level to be assigned, the lower level will be assigned.

## **2-11. Duration of classification**

Information will be declassified as soon as it no longer meets the standards for classification. Information will remain classified as long as it is in the interest of national security and meets the criteria stated in this regulation. At the time an item of information is originally classified, the original classifier must decide the length of time the information will require classification and select an appropriate declassification date or event. The term “time or event phased declassification date,” used for acquisition programs, is also synonymous with the term “declassification date” as used in this regulation. The declassification date indicates when the information no longer requires protection in the interests of national security. When deciding on the declassification date or event, the following options are the only ones available to the OCA:

a. At the time of original classification, the original classification authority will attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The OCA will attempt to determine a date, within ten years from the date of classification, upon which the information can be automatically declassified. If that is not possible, they will attempt to determine a specific event, reasonably expected to occur within 10 years, that can be set as the signal for automatic declassification of the information. This is referred to as the “ten-year rule.” The date or event will not exceed the time frame in subparagraph c, below.

b. If information has originally been assigned a date or event for declassification of ten years or less, in accordance with subparagraph a above, and the OCA later has reason to believe longer protection is required, the classification can be extended for successive periods of up to ten years at a time, not to exceed the time period in subparagraph e, below, where applicable.

c. If unable to determine a date or event that is ten years or less, the OCA will assign an exemption designation to the information, if the information qualifies for exemption from automatic declassification in ten years. This could be done if the unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, if specific information requires a period beyond 10 years from the date of original classification, and the release of the information could reasonably be expected to result in one or more of the following:

(1) Reveal an intelligence source, method, or activity, or a cryptologic system or activity.

(2) Reveal information that could assist in the development or use of weapons of mass destruction.

(3) Reveal information that could impair the development or use of technology within a United States weapon system.

(4) Reveal United States military plans or national security emergency preparedness plans.

(5) Reveal foreign government information.

(6) Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than ten years.

(7) Impair the ability of responsible United States government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized.

(8) Violate a statute, treaty, or international agreement. Note: When used, these eight exemption categories are either completely written out or referred to by their reference number preceded by the letter "X." For example, "Violate a statute, treaty, or international agreement" or "X8." See paragraph 4-10 for further details on exemption marking.

d. Information marked for an indefinite duration of classification under prior orders, for example, "Originating Agency's Determination Required" (OADR), or information classified under prior orders that contain no declassification instructions, will be declassified in accordance with chapter 3 of this regulation. The term OADR will no longer be used. When an exemption category is selected, there is no requirement to select a specific date or event for declassification at the time of original classification. In those cases in which the original classifier does not select a declassification date, the following will apply:

(1) The information, if placed in records that have been determined to have permanent historical value under Title 44, USC (see "permanent" files under AR 25-400-2), will be automatically declassified in 25 years from the date of original classification, unless specifically exempted or unless this policy is changed before that time.

(2) The information, if not placed in such records (mentioned in subparagraph (1) above), will remain classified until destroyed, or until the OCA determines a change in classification.

e. For information in records determined to have permanent historical value, successive extensions may not exceed a total of 25 years from the date of the information's origin. Continued classification of this information is governed by the automatic declassification provisions of this regulation contained in chapter 3.

f. Decisions to extend classification must take into account the potential difficulty of notifying holders of the extension, including the possible inability to ensure continued, uniform protection of the information. Officials who decide to extend a declassification date are responsible for notifying all known holders of the information of the decision and for obtaining assurance from those holders that notification has been made to organizations that were provided the information under further dissemination by those holders.

## **2-12. Communicating the Classification Decision**

An original classification authority who has made a decision to originally classify information is responsible for communicating that decision to persons who will likely be in possession of that information. This will be accomplished by issuing classification guidance, discussed in section V of this chapter, or by making sure that a document containing the information is properly marked to reflect the decision. Marking requirements for classified material, including page and paragraph markings, are covered in chapter 4 of this regulation.

## **2-13. Compilation**

Generally, a compilation of unclassified items of information is not classified. In unusual circumstances, compilation of items of information that are individually unclassified can be classified if the compiled information reveals an additional association or relationship that matches criteria for classification as described in paragraph 2-8 of this regulation. Classification by compilation will be fully supported by a written explanation that will be provided on, in, or with, the material containing the information. An OCA must be consulted if guidance is required concerning whether or not the compilation results in classification.

## **2-14. Acquisition Systems**

Classification and safeguarding of information involved in the DOD acquisition process will conform to the minimum standards of this regulation, as well as the requirements of DODD 5000.1 and DOD Instruction (DODI) 5000.2 (or successor directives and instructions). The term "time or event phased declassification date", used for acquisition systems, is synonymous with the term "declassification date" used in this regulation.

## **2-15. Limitations and prohibitions**

EO 12958 and the Atomic Energy Act of 1954 provide the only basis to classify information. Information will only be classified when it requires protection in the interest of national security as specified in this regulation. Classification cannot be used to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, agency, or to restrain competition. Basic scientific research and its results can be classified only if it clearly relates to the national security. Section VI of this chapter covers information that is a product of non-government research and development, that does not incorporate, or reveal, classified information to which the producer, or developer, was given prior access.

## **Section IV**

### **Security Classification Guides**

#### **2-16. Policy**

A Security Classification Guide (SCG) will be issued for each system, plan, program, or project in which classified information is involved. Agencies with original classification authority will prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides will conform to standards contained in directives and regulations issued under EO 12958 and this regulation.

#### **2-17. Content**

Security classification guides will, at a minimum, include the following information:

- a. Identify specific items or elements of information to be protected and the classification level to be assigned each item or element. When deemed useful, specify the items or elements of information which are unclassified or which were previously classified and now are declassified.
- b. Provide declassification instructions for each item or element of information, to include the applicable exemption category for information exempted from declassification within ten years. See paragraph 2-11 for exemption categories.
- c. Provide a concise reason for classification for each item, element, or category, of information which, at a minimum, cites the applicable classification category or categories from section 1.5 of EO 12958 and that are listed in paragraph 2-8 of this regulation.
- d. Identify any special handling caveats or warning notices or instructions, which apply to the items, elements, or categories of information.
- e. Identify by name, or personal identifier, and position title, the OCA approving the guide, and the date of the approval. A personal identifier is any grouping of letters or numbers used in an organization code that the command uses to identify a particular position. Classification guides will normally be signed by the OCA and, where that is the case, the name and position title, rather than the personal identifier and position title, will be used.
- f. Provide a point of contact, with telephone number, for questions concerning the guide, challenges to classification, and suggestions for improvement. Provide a statement in the guide encouraging personnel to informally question the classification of information before resorting to a formal challenge. Provide an address for formal classification challenges.

#### **2-18. Approval, distribution, and indexing**

- a. Security classification guides will be personally approved in writing by the original classification authority who is authorized to classify information at the highest level designated by the guide, and who has program support or supervisory responsibility for the information or for the command's information security program.
- b. Security classification guides will be distributed to those commands, contractors, or other activities expected to be derivatively classifying information covered by the guide.
- c. One paper document copy of each approved SCG (less those for SAPs or programs involving SCI) and its changes will be sent to the Director of Freedom of Information and Security Review, Office of the Assistant Secretary of Defense. Also, one copy, in paper document (hard copy) and/or automated format (soft copy), will be sent to the Army Declassification Special Program Office. See AR 380-381 for guidance on distribution of classification guides for SAPs, and AR 380-28 for guidance on SCI programs.
- d. Two copies of each guide, other than those covering SAPs or SCI information, will be provided to the Administrator, Defense Technical Information Center (DTIC). Each guide furnished to DTIC must bear the appropriate distribution statement required by DODD 5230.24. Security classification guides issued under this regulation, will be indexed in the DOD Index of Security Classification Guides (DOD 5200.1-1). The originator of the guide will submit DD Form 2024 (DOD Security Classification Guide Data Elements) to the Administrator, DTIC, upon approval of the guide. If the originator determines that listing the guide in DOD 5200.1-1 would be inadvisable for security reasons, issuance of the guide will be separately reported, with an explanation of why the guide cannot be listed, to the Director, Special Programs, ODTUSD(P)PS, along with a separate memorandum to DAMI-CH. Report Control Symbol DD-C31 (B&AR) 1418 applies to the reporting requirements of this paragraph.

#### **2-19. Review, revision, and cancellation**

- a. Security classification guides will be revised whenever necessary to promote effective derivative classification. When a guide is revised or reissued, and a specific date was selected for declassification instruction, computation of declassification instructions will continue to be based on the date of the original classification of the information, and not on the date of the revision or re-issuance. Guides will be reviewed by the originator for currency and accuracy at least once every five years, or if concerning a defense acquisition program, prior to each acquisition program milestone, whichever occurs first. Changes identified in the review process will be promptly made. If no changes are

required, the originator will advise the Administrator, DTIC, and DAMI-CH in writing, and the record copy of the guide will be so annotated with the date of review.

b. Guides will be cancelled only when:

- (1) All information specified as classified by the guide has been declassified;
- (2) When the system, plan, program, or project classified by the guide has been cancelled, discontinued, or removed from the inventory and there is no reasonable likelihood that information covered by the guide will be involved in other classified programs or will be the subject of derivative classification; or
- (3) When a major restructure has occurred as the information is incorporated into a new classification guide and there is no reasonable likelihood that information covered by the guide will be the subject of derivative classification.

c. Impact of the cancellation on systems, plans, programs, and projects provided to other nations under approved foreign disclosure decisions, and impact of such decisions on existing U.S. SCGs of similar systems, plans, programs, or projects, will be considered in the decision. When a classification guide is cancelled because the system, plan, program, or project has been cancelled, discontinued, executed, or removed from the inventory, the information covered by the guide is not automatically declassified. That decision rests with the OCA and authorized declassification authorities within the Army. Upon cancellation of a guide, the OCA, or other designated declassification official, with the concurrence of the OCA, will consider the need for publication of a declassification guide. In place of a separate declassification guide, declassification guidance can be included in a classification guide for a similar, current system, plan, program, or project.

d. Revision, re-issuance, review, and cancellation of a guide will be reported to DTIC on DD Form 2024 as required for new guides. Copies of changes, reissued guides, and cancellation notices will be distributed as required for new guides as stated in paragraph 2-18 of this regulation.

## **Section V**

### **Non-Government Information**

#### **2-20. Policy**

Information that is a product of contractor or individual Independent Research and Development (IR&D) or Bid and Proposal (B&P) efforts, conducted without prior or current access to classified information associated with the specific information in question, cannot be classified unless:

- a. The U.S. Government first acquires a proprietary interest in the information.
- b. The contractor, conducting the IR&D/B&P, requests the U.S. Government activity to place the information under the control of the security classification system, without relinquishing ownership of the information.

#### **2-21. Classification determination**

- a. The individual or contractor conducting an IR&D/B&P effort could believe that information, generated without prior access to classified information, or current access to classified information, associated with the specific information in question, might require protection in the interest of national security. The contractor would then safeguard the information and submit it to an appropriate Army, or other U.S. Government activity, for a classification determination.
- b. The Army command receiving such a request will issue security classification guidance as appropriate if the information is to be classified. If the information is not under that command's OCA, the command will refer the matter to the appropriate OCA or inform the individual or contractor to take that action. The information will be safeguarded until the matter has been resolved.
- c. The Army command that holds classification authority over the information will verify whether or not the individual or contractor is cleared and has authorized storage capability. If not, the appropriate contracting authority for the command will advise whether or not to process clearance action.
- d. If the individual or contractor refuses to be processed for a clearance, and the government does not acquire a proprietary interest in the information, the information cannot be classified.

#### **2-22. Classification challenges**

- a. If authorized holders of information have substantial reason to, in good faith, believe that the information is improperly or unnecessarily classified, they will communicate that belief through their command security manager, to the OCA of the information, to bring about any necessary correction. This can be done informally, or by submission of a formal challenge, to the classification as provided for in EO 12958 and this regulation. Informal questioning of classification is encouraged before resorting to formal challenge. Commanders will establish procedures through which authorized holders of classified information within their Commands, can challenge a classification decision, and will ensure that Command personnel are made aware of the established procedures. An authorized holder is any person who has been granted access to specific classified information being challenged. OCAs will establish written procedures through which authorized holders of classified information can challenge classification decisions. At a minimum, security classification guides will contain a point of contact to informally communicate classification challenges and an address to communicate formal classification challenges. EO 12958 establishes the Interagency Security Classification

Appeals Panel (ISCAP). One of the roles of the panel is to decide upon appeals by authorized holders of the information who have made a formal classification challenge as described in this section. See section 5.4, EO 12958, a reprint of which is found at appendix B of this regulation, for more details on the composition and function of this panel.

(1) Formal challenges to classification, made under this subsection, will include a sufficient description of the information being challenged, to permit identification of the information and its classifier, to include the OCA, where known, with reasonable effort. Challenges to classification made by Army personnel will include the reason why the challenger believes that the information is improperly or unnecessarily classified. Use of DA Form 1575 (Request for/ or Notification of Regrading Action) may be used to make a formal challenge. The challenge request should be unclassified, if possible. The classification determination of the OCA will be upheld and carried forward until otherwise determined by the appropriate authorized official.

(2) Commanders will make sure that no retribution is taken against any personnel for making a challenge to a classification.

b. The following will be established by each OCA:

(1) A system for processing, tracking, and recording formal challenges to classification. The system used will differentiate the classification challenges with other reviews for possible declassification (for example, FOIA requests). Requests for information made under the FOIA will be handled as directed by AR 25-55.

(2) The OCA will provide a written response to the challenge within 60 calendar days following the receipt of the challenge. If the OCA cannot respond fully to the challenge within 60 calendar days from receipt, the challenge will be acknowledged and an expected date of response provided. This acknowledgment will include a statement that, if no response is received within 120 calendar days following receipt of the challenge, the challenger has the right to forward the challenge to ISCAP. The challenger can also forward the challenge to the ISCAP if the OCA has not responded to an internal appeal within 90 calendar days of receipt. An internal appeal is when the challenge comes from DA personnel to a Department of the Army OCA. An information copy of the request for appeal, submitted by DA personnel, whether or not to a Department of the Army OCA, will be sent to the original classification authority.

(3) If the challenge is denied and the original classification authority determines that the information is properly classified, the OCA will advise the challenger of the right to appeal the decision. The first level of appeal will be to the first superior general officer in the chain of command of the original classification authority. That general officer will either rule on the appeal, in an impartial manner, or will designate an impartial official, or panel of officials, knowledgeable in the subject matter of the information being challenged, to decide upon the appeal. Both the challenger and the OCA will be advised of the appeal decision. The same time frames and notification to the challenger, stated in subparagraph b, above, apply to the first level of the appeal procedure. If, as a result of the first level of appeal, the challenge is denied, and the appeal authority determines that the information is properly classified, the appeal authority will advise the challenger of the right to appeal the decision to the ISCAP. The Director of the ISOO serves as the Executive Secretary of the ISCAP. The correct address to furnish the challenge for appeals to that panel is to the Executive Secretary of the Interagency Security Classification Appeals Panel, c/o ISOO. As of the publication date of this regulation, the mailing address for ISOO is: Information Security Oversight Office (ISOO), National Archives and Records Administration, 700 Pennsylvania Avenue, NW, Room 5W, Washington D.C. 20408.

(4) If a challenge is received concerning information that has been the subject of a challenge, within the preceding two years, or which is the subject of pending litigation, the original classification authority need not process the challenge. The OCA has the option of whether or not to process the challenge. If the challenge is not processed, the challenger will be informed of the situation and that the matter may be appealed to the ISCAP.

(5) If a challenge is received concerning information that has been classified by another OCA within the Army, or by another agency in the U.S. Government, the challenger will be informed of this fact and directed to resubmit the challenge to the appropriate official.

(6) If a challenge is received concerning information classified by a foreign government or international organization, the receiver of the challenge will forward the request for classification review to the appropriate foreign government agency that classified the information. The request to the foreign government for classification review will state that within the United States it is the procedure to respond to these challenges or notify the challenger within 60 calendar days of receipt of the request, and that it would be appreciated if this same response time could be observed. The correspondence to the foreign government will also inquire if there is any appeal authority, and if so, that this authority be listed in the response if the challenge is denied. The challenger will be advised of this referral, if applicable. Army OCAs will be responsive to such informal inquiries and will recognize that the Army has no control over a timely, or lack of, response from the foreign government. The reply from the foreign government, upon receipt, will be forwarded by the requester to the challenger.

c. Information that is the subject of a classification challenge will continue to be classified and appropriately safeguarded until a decision is made to declassify it.

must continue to be controlled at their prior classification or sensitivity level. Purging or sanitizing of media means to erase or overwrite, totally and unequivocally, all information stored on the media. Declassifying of media refers to the administrative action taken after it has been purged. Declassifying is required when the media must leave the facility under the control of uncleared personnel; for example, for maintenance operations.

b. The decision to declassify media will be made only after comparing the inherent risks (in the Magnetic Media Remanence Guide – Rainbow Series) with the financial or operational benefit of media declassification. For example, destruction of media is normally more appropriate than declassification and reuse, given the low cost of the media.

c. Media can be declassified only after purging. The appropriate ISSO must verify that the technique chosen for purging (or sanitizing) meets applicable requirements. Additionally, the ISSO must establish a method to periodically verify the results of the purging. As a minimum, a random sampling will be taken to verify each purge.

d. Degaussing must be accomplished using NSA-approved equipment from the Degausser Products List of the Information Systems Security Products and Services Catalogue. Information on degaussers is available through the information systems security management structure. Some listed products may be used only to degauss magnetic media that has coercivity no greater than 350 oersteds (also known as type I media), while others are approved for media with coercivity no greater than 750 oersteds (also known as type II media). Certain tape media have a coercivity greater than 750 oersteds (also known as type III media) and cannot, at this time, be completely degaussed. (See AR 380-19 for more information.)

e. A CD-ROM will be destroyed by scratching both surfaces with an abrasive substance, to render the CD unreadable, prior to breaking the CD into numerous pieces with an impact device, such as a hammer.

f. Storage media containing Sensitive Compartmented Information (SCI) will be handled as stated in AR 380-19, and media containing Special Access Program (SAPs) material will be handled as stated in AR 380-381.

## **Chapter 4 Marking**

### **Section I Marking Documents**

#### **4-1. Purpose and policy**

Marking is the principal means of informing holders of classified and sensitive information of its classification/sensitivity level and protection requirements. Within the Department of the Army, classified and sensitive material will be identified clearly by marking, designation, electronic labeling, or if physical marking of the medium is not possible, by some other means of notification. The term “marking” as used in this regulation is intended to include all these methods of notification. The term “document” as used in this section is meant to apply to all classified and unclassified material, no matter what form (paper, electronic, etc.) it is in. Classification/sensitivity markings must be conspicuous. Original and derivative classifiers are responsible for application of the appropriate classification/sensitivity markings. The requirements for marking information and material within the intelligence community are a little different. These requirements can be found in appendix D, of this regulation, and successor Director of Central Intelligence Directives (DCID). The requirements of this chapter do not apply to the marking of security containers. The only markings allowed on security containers are those outlined in paragraph 7.8 of this regulation. Marking serves these purposes:

- a. Alerts holders to the presence of classified and sensitive information.
- b. Identifies, as specifically as possible and feasible, the exact information needing protection.
- c. Indicates the level of classification/sensitivity assigned to the information.
- d. Provides guidance on downgrading (if any) and declassification.
- e. Gives information on the source(s) and reason(s) for classification of the information.
- f. Warns holders of special access, control, dissemination, or safeguarding requirements.

#### **4-2. Exceptions**

a. Public Media — Classification and/or other security markings will not be applied to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium. If such an article is evaluated to see if it contains classified and/or sensitive information, the results of the review will be properly marked, if classified and/or sensitive, and will be kept separate unless both the article and the results of the review are protected (stored and otherwise safeguarded as classified/sensitive information). DA personnel will neither confirm nor deny the presence of classified and/or sensitive information or the accuracy of such information when that information has appeared in the public media.

b. Confidential Source or Relationship — Classified documents and material will be marked in accordance with this regulation unless the markings themselves would reveal a confidential source or relationship not otherwise evident in the document, material, or information.



c. Restricted Data/Formerly Restricted Data — The marking requirements for the date or event for declassification do not apply to documents or other material that contain, in whole or part, RD or FRD information. Such documents or other material or portions thereof will not be declassified without approval of the Department of Energy with respect to Restricted Data or Formerly Restricted Data information, and with respect to any national security information contained therein, the approval of the originating agency.

#### 4-3. Requirements

General requirements are shown in this section. Each of these requirements is explained in more detail in a separate section of this chapter. Figures 4-1 through 4-13, at the end of this chapter, provide examples of the most typical situations. These figures are not intended to cover all situations. Material other than paper documents require the same markings and must have the same information either marked on it or made available to holders by other means of notification. While not a requirement, the holder of an improperly marked classified document should contact the document originator to obtain correct markings. Classified and sensitive material will bear the following markings:

- a. The overall (highest) classification/sensitivity of the information.
- b. The command, office of origin, date, and if not evident by the name of the command, the fact that the document was generated by the Department of the Army.
- c. Identification and date of the specific classified information in the document and its level of classification (page and portion markings).
- d. Identification of the source(s) of classification ("Classified by" or "Derived from" line), and, for originally classified information, the concise reason(s) for classification. In cases of derivative classification, the reason(s) the source of the classified portion(s) is/are derived from.
- e. Declassification instructions ("Declassify on" line), and downgrading instructions, if any downgrading applies.
- f. Warning and sensitivity notices and other markings, if any, that apply to the document.

#### 4-4. Overall classification marking

Classified and sensitive documents will be marked to show the highest classification/sensitivity of information contained in the document. For documents containing information classified at more than one level, the overall marking will be at the highest level. For example, if a document contains some information marked "SECRET" and some information marked "CONFIDENTIAL", the overall marking would be "SECRET". This marking must be conspicuous enough to alert personnel handling the material that it is classified and must appear in a way that will distinguish it clearly from the text of the document. The overall classification/sensitivity will be conspicuously marked, stamped, or affixed (with a sticker, tape, etc.), top and bottom, on the front and back covers (if the document has covers), on the title page (if there is one), and on the first page, in letters larger than those on the rest of the page. If it is not possible to mark classification/sensitivity in letters which are larger than the rest of the text (for example, on covers of documents or graphics), apply classification/sensitivity markings in any manner that is immediately noticeable. To promote reproducibility, classification/sensitivity and associated markings will be applied in black or other dark ink. The use of red ink is discouraged. If the document or other material has no front cover, the first page will be the front page. If it has a cover, the first page is defined as the first page that can be seen when the cover is turned back or opened. In some documents, the title page and first page can be the same.

#### 4-5. Date, command, office of origin, and agency

Classified and sensitive documents will be marked on the face of the document with the date of the document, the command that originated it, the office or agency which originated it, and "U.S. Army" or "Army" if it is not clear from the name of the command that it is a DA activity originating the document. This information will be clear enough to allow the recipient of the document to contact the preparing office if questions or problems about classification arise.

#### 4-6. Page and portion marking

Each classified and/or sensitive document must show, as clearly as possible and feasible, which information in it is classified and/or sensitive and at what level. That will be done in the following manner:

- a. Each interior page of a classified and/or sensitive document (except blank pages) will be conspicuously marked, top and bottom, with the highest classification/sensitivity of the information on the page. The marking must be conspicuous enough that it is clearly distinguishable from the regular text of the document. Blank interior pages are not required to be marked. This is the preferred method of page marking. As an alternative to marking pages according to individual page content, the interior pages can be marked with the highest overall classification/sensitivity of information within the document. If this alternative method is used, portion marking must be used and cannot be excepted as described in paragraph 4-6c, below.
- b. Each section, part, paragraph, and similar portion of a classified and/or sensitive document will be marked to show the highest level of classification/sensitivity of information it contains, or that it is UNCLASSIFIED. "Portion marking" is the term used to meet this requirement. The term "paragraph marking" is generally used interchangeably with "portion marking". Whether referred to as portion or paragraph marking, the term includes the marking of all portions of a document, not just paragraphs. When deciding whether a subportion (such as a subparagraph) will be

marked separately as a "similar subportion", the deciding factor is whether or not the marking is necessary to eliminate doubt about the classification/sensitivity of its contents. Unless the original classification authority or originator of the document indicates otherwise on the document, each classified and/or sensitive portion of a document will be presumed to carry the declassification instructions (date, event, or exemption category) of the overall document.

(1) Each portion of text will be marked with the appropriate abbreviation ("TS" for TOP SECRET, "S" for SECRET, "C" for CONFIDENTIAL, or "U" for UNCLASSIFIED), placed in parentheses immediately before the beginning of the portion. If the portion is numbered or lettered, the abbreviation will be placed in parentheses between the letter or number and the start of the text. Some agencies permit portion marking at the end of the portion, rather than at the beginning. The Department of the Army does not. When extracts from non-DA documents are made and incorporated into DA documents, the portion marking will be placed at the beginning of the portion.

(2) Portions containing Restricted Data (RD) and Formerly Restricted Data (FRD) will have abbreviated markings ("RD" or "FRD") included with the classification marking, for example, "(S-RD) or (S-FRD)". Critical Nuclear Weapons Design Information (CNWDI) will be marked with an "N" in separate parentheses following the portion marking, for example, "(S-RD)(N)".

(3) The abbreviation "FOUO" will be used in place of "U" when a portion is UNCLASSIFIED but contains "For Official Use Only" information. AR 25-55 contains the definition and policy application of FOUO markings. See chapter 5, of this regulation, for further guidance, as well.

(4) Portions of DA documents containing foreign government or NATO information will include identification of the foreign classification in the marking in parentheses. For example, "(UK-S)" for information classified "SECRET" by the United Kingdom; and "(NATO-C)" for North Atlantic Treaty Organization (NATO) information classified as "CONFIDENTIAL".

(5) Paragraph 5-410, DODD 5200.1-R stated that the caveat "NOFORN" will no longer be used. This has since been rescinded. Effective with the release of Director of Central Intelligence Directives (DCID) 1/7 (see app D) and DCID 5/6, both dated 30 June 1998, the use of "US ONLY," to mark information that must be restricted to U.S. nationals, will cease. Until revoked, this type of information will be marked "NOFORN." This applies to all media, including hard copy, digital, and graphic.

(6) The subject and title of classified documents will be marked to show the classification of the information in the subject or title. The same abbreviations ("TS", "S", "C", "U", or "FOUO") will be used but the abbreviations will be placed in parentheses at the end of the subject or title.

(7) Charts, graphs, photographs, illustrations, figures, tables, drawings, and similar portions will be marked with the unabbreviated classification/sensitivity, such as "UNCLASSIFIED", based on the level of classified and/or sensitive information revealed. The marking will be placed within the chart, graph, etc., or next to it, such as on the frame holding the document. Captions and titles of charts, graphs, etc., will be marked as required for text portions (such as paragraphs) and will be placed at the beginning of the caption or title.

(8) See appendix D for an explanation of marking certain intelligence control markings (for instance, ORCON and PROPIN). Portion marking of those intelligence control markings will follow the policy as stated in DCID 1/7 and successor directives.

(9) See appendix I for an explanation of marking Special Access Programs (SAPs) material.

c. If an exceptional situation makes individual marking of each paragraph or other portion clearly impracticable, a statement can be substituted describing the fact that portion markings were not used, and which portions are classified and/or sensitive and their level of classification/sensitivity. Such a statement will identify the information as specifically as would have portion markings. For classification by compilation, the statement required by paragraph 2-13 meets this requirement.

d. Documents containing information classified by compilation will be marked as follows:

(1) If portions, standing alone, are UNCLASSIFIED, but the document is classified by compilation (see para 2-13), mark the portions as "(U)" and the document and pages with the classification of the compilation. You must also add an explanation of the classification as required in paragraph 2-13 of this regulation.

(2) If individual portions are classified and/or sensitive at one level, but the compilation results in a higher classification/sensitivity, mark each portion with its own classification/sensitivity and mark the pages, and the overall classification/sensitivity of the document, with the higher classification/sensitivity of the compilation. An explanation of the classification/sensitivity by compilation is required to be placed in the document, preferably on the cover or title page.

(3) DAMI-CH will be contacted for guidance on submission of waivers or exceptions to policy concerning the marking of documents classified and/or sensitive by compilation.

#### **4-7. Sources of classification - overview**

Each classified document will be marked with the source of the classification. For originally classified documents, that identification will be preceded by the term "Classified by". In cases of derivative classification, the source of classification is derived from either:

(1) A classification guide or guidance.



(2) A classified source document that was used to extract, summarize, restate, or paraphrase information from the source document into the new document.

(3) When compilations of items of information that are individually unclassified can be classified if the compilation reveals an additional association or relationship that matches criteria for classification pursuant to paragraph 2-8 of this regulation. For derivatively classified documents, the term "Derived from" will precede the identification of the source of classification. This is a change from previous policy. Previous policy required the use of the "Classified by" line for both originally and derivatively classified documents. Current policy requires the use of the "Classified by" line only for original classification documents and combination original and derived documents, and requires the use of the "Derived from" line for only wholly derived classified documents. See chapter 2 for a further explanation of the differences between, and requirements for, originally and derivatively classified documents.

#### **4-8. Sources of classification – procedures**

a. Originally classified documents. Each originally classified document will have a "Classified by" line placed on the face of the document. The "Classified by" line will identify the original classification authority responsible for classification of the information contained in the document. The OCA will be identified by name or personal identifier (see paragraph 2-17e for an explanation of the term "personal identifier"), and position title. If the information required to be included in the "Classified by" line would reveal classified information not evident from either the rest of the document or not evident from the face of the document, the "Classified by" line will be completed with an UNCLASSIFIED identification (such as an UNCLASSIFIED personal identifier) that can be traced through secure channels.

b. Derivatively classified documents. Each derivatively classified document will have a "Derived from" line placed on the face of the document. The term "Classified by" will not be used on classified documents that are wholly derivative. The "Derived from" line will be completed as follows:

(1) If all the information was classified using a single security classification guide (or guidance) or only one source document, identify the guide or the source document on the "Derived from" line. Include the date of the guide or document. If using a source document that cites a guide as classification authority, use the guide rather than the source document on the "Derived from" line.

(2) If more than one security classification guide, source document, or combination of guide(s) and document(s) provided the derivative classification guidance, use the term "Multiple Sources" on the "Derived from" line. If "Multiple Sources" is placed on the "Derived from" line, a record of the sources will be maintained on or with the file or record copy of the document. Whenever feasible, this list should be included with all copies of the document. If the document has a bibliography or list of references, that can be used as the listing of sources as long as it is annotated to delineate the sources of classification from the other references. A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" will cite the source document on its "Derived from" line rather than the term "Multiple Sources". (For example, "Derived from: Headquarters, Department of the Army Report, Security 2001, an Army Odyssey, 10 February 1997, Office of the Deputy Chief of Staff for Intelligence (DAMI-CH).")

c. Combination of original and derivative classification. There can be situations in which some information in a document is originally classified at the time of preparation of the document and some information is derivatively classified. In those cases, mark the document with a "Classified by" line and place "Multiple Sources" on the line. For the information originally classified in the document, the OCA will be included in the list of sources required in paragraph 4-8b(2).

#### **4-9. Reason for original classification**

Each originally classified document will bear a concise line that describes the reason for the decision to classify. This requirement applies only to originally classified documents and does not apply to derivatively classified documents. The "Reason" line will not be used on wholly derivatively classified documents. The "Reason" line is placed between the "Classified by" line and the "Declassify on" line. The reason(s) to classify relates to the categories of what can be classified, as specified in paragraph 2-8. The "Reason" line will either:

a. State one or more of the reasons listed in paragraph 2-8. For example: "Reason: Military plans, weapons systems, or operations"; or "Reason: Foreign government information"; or "Reasons: Military plans, weapons systems, or operations; and foreign government information".

b. State the reason in terms of listing the number "1.5" followed by the letter, in parentheses, that corresponds with the appropriate category or categories of information listed in section 1.5 of E.O. 12958. This is the same list shown in paragraph 2-8 of this regulation. For example: If the information is classified because it concerns military plans, weapons systems, or operations, mark the document: "Reason: 1.5(a)". If the document is classified because it contains foreign government information, mark the document: "Reason: 1.5(b)". If the document is classified for both reasons, mark the document: "Reasons: 1.5(a) and 1.5(b)."

c. For those cases in which the document contains both originally classified and derivatively classified information,

state the reason(s), as described in subparagraph a or b of this paragraph, and add the words, "and derivatively classified source" or "and derivatively classified sources", where more than one derivative source document is used.

#### 4-10. Declassification instructions—"Declassify on" line

Each classified document (except those containing RD and FRD) will be marked on the face of the document with a "Declassify on" line, with instructions for the declassification of the information. This applies for all classified documents, both originally and derivatively classified. The "Declassify on" line will be completed as follows:

a. *Originally classified documents.* If all the classified information is the product of original classification, the OCA will specify the instruction on the "Declassify on" line. The instruction will specify either a date for declassification, an event for declassification, or an indication that the information is exempt from declassification within ten years.

(1) If any information in the document has been exempted from declassification within ten years, referred to as the "Ten Year Rule," the "Declassify on" line will be completed with an "X" followed by a number or numbers which show the applicable exemption category or categories from paragraph 2-11c. There is no alternative to listing the category in this manner. For example, a document containing information requiring classification beyond ten years because it would reveal information that would impair the development or use of technology within a U.S. weapon system (category number 3 under paragraph 2-11c) would be marked: "Declassify on: X3". As another example, a document containing information requiring classification beyond ten years because it reveals U.S. military plans (category number 4 under paragraph 2-11c) would be marked "Declassify on: X4". Note: Listing the exemption category number rather than the words describing the category is the preferred method of citing declassification exemption instructions within DOD.

(2) For cases in which it is possible for the Original Classification Authority to select a date or event for declassification at a point occurring more than ten years in the future, the date or event would follow the exemption category number. An example is "Declassify on: X3, 11 November 2011". There can be cases in which it is not possible for the OCA to select a future date or event for declassification. In those cases, only the exemption category will be listed. Examples for those cases, such as "Declassify on: X3", are shown in subparagraph (1), above.

(3) If more than one exemption applies, the OCA will list each exemption. For example, a document originally classified beyond ten years because it would reveal information that would impair the development or use of technology within a U.S. weapons system (exemption category 3) and that also contains foreign government information (exemption category 5) would be marked, "Declassify on: X3,5".

(4) Regardless of the exemption category used, or whether or not a date or event for declassification has been selected, the information can be subject to the automatic declassification provisions of the current EO or statute on classification. EO 13142, the most recent amendment to EO 12958, section 3.4, requires all classified information contained in records that will be more than 25 years old on 17 October 2001, and have been determined to have permanent historical value under Title 44, USC, to be declassified on 17 October 2001, unless the information has been exempted. The current criteria for exemption for 25 year old information is contained in chapter 3 of this regulation and in section 3.4 of EO 12958. It is impossible to predict what criteria will apply to any future automatic declassification programs. It is important for OCAs to carefully select the appropriate exemption category (with or without a declassification date or event) for currently classified information. Future automatic declassification programs might use a formula to convert current exemptions to future criteria used in reviewing old classified documents. If more than one exemption applies, it is important to list each exemption category.

b. *Derivatively classified documents.* In a derivatively classified document there may be one source from which the classification is derived, or there may be several sources. The source may have been classified after 14 October 1995 (the date the requirements of EO 12958 went into effect) and reflects the current system of conveying declassification instructions. The source may have been classified prior to 14 October 95 under the former system in which the use of the term Originating Agency Determination Required (OADR) was often used. Or, the source may have been classified after 14 October 95 but still reflects the former system of conveying declassification instructions. Even in cases in which only one source document is used, and often in cases in which several sources are used, different declassification instructions may apply to the various items of information in the document being created. To ensure that all the information in the document is protected for as long as necessary, the most restrictive declassification instruction that applies to any of the information in the document will be placed on the "Declassify on" line. The term "most restrictive" means the latest date or event, or the date or event furthest in the future. Throughout this regulation the term "OADR" is used strictly because there are documents out there with this term. The term "OADR" is no longer authorized.

(1) If all the information in the document has the same declassification instruction (i.e. same date, event, or exemption category or categories), and that instruction is an allowable option under the new policy contained in EO 12958 as stated in this regulation, place that instruction on the "Declassify on" line. The allowable options are:

(a) A date or event for declassification within 10 years from original classification.

(b) An exemption category for information classified beyond 10 years (see paragraph 4-10a) such as "X4." When an exemption category is used, it may or may not be followed by a declassification date or event, depending upon whether the original classification authority has selected a declassification date or event.

(c) For documents that will be over 25 years old on 17 October 2001, and are contained in records that have been determined to have permanent historical value under Title 44 of the USC, an exemption category or categories as shown in chapter 3.

(d) The source may be marked with one of the indefinite markings used before the term "OADR" was authorized. In such cases, any information with indefinite declassification instructions will be treated as though it were marked as "OADR".

(e) There are two different lists of exemption categories. One list applies to information that requires classification for more than 10 years. This list is contained in paragraph 2-11c. The other list applies to information contained in the exempted file series list and that will be more than 25 years old by 17 October, 2001. That list is contained in paragraph 3-6e.

(2) If all the information in the document has been extracted from a document created before 14 October 1995 (the effective date of EO 12958) and was marked "OADR", place the statement "Source marked OADR" on the "Declassify on" line, followed by the date of the document after the words "Date of Source". For example, a derivative classifier extracts classified information from a document dated 3 June 1992 and marked "OADR". The newly created document containing that extract will be marked, "Declassify on: Source marked OADR; Date of Source: 3 June 1992." When using several sources of information marked "OADR", the "Date of Source" line will reflect the most recent date (the document with the latest date). For example, one source is dated 2 August 1993 and one is dated 1 September 1995. In this case, the newly created derivatively classified document will be marked:

Derived from: Multiple Sources

Declassify on: Source marked OADR;

Date of Source: 1 September 1995

(3) No matter what combination of indefinite declassification instructions and document dates used as sources to derivatively classify the document, the document originator will only select the source document with the most recent date and this will determine the date to place on the "Date of Source" line. Follow this policy for all cases involving information classified under previous Executive Orders that contain indefinite declassification instructions. Follow this policy for all cases involving information extracted from a document created after 14 October 1995 that was mistakenly marked as OADR. Where practical and feasible, notify the originator of that mistakenly marked document of the outdated declassification instructions and obtain the current correct markings.

(4) If the document is classified by more than one source ("multiple sources") and different declassification instructions apply, the derivative classifier will place the most restrictive declassification instruction on the "Declassify on" line. The most restrictive declassification instruction is the date or event that will occur farthest in the future (the longest date from now). The following applies:

(a) If declassification dates are specified for all of the sources of information used in the document, place the latest date (date farthest in the future) on the "Declassify on" line. For example, in creating a new document, information is extracted from documents marked for declassification on 20 March 1998, 1 June 2002, and 3 April 2009. The newly created document will be marked: "Declassify on: 3 April 2009".

(b) If the sources of classification are a combination of a date or dates with an event or events, the declassification instruction will reflect whichever date and event occurs later (date or event farthest in the future). If the date of the event(s) is unknown, the declassification instruction will reflect the most restrictive date and latest occurrence of the event(s). For example, one source specifies a declassification date of 11 November 2011, and the other a declassification event upon execution of operations. In this case, the document will be marked: "Declassify on: 11 November 2011 or execution of operations, whichever is later".

(c) If any of the information in the document does not have a specific date or event for declassification, the originator of the derivatively classified document will apply the most restrictive declassification instruction, according to the following:

1. When using information classified under a previous EO, any information with an indefinite declassification (such as Group 3 or OADR) is treated as if it were marked "OADR" and marked as specified in paragraph 4-9b.

2. When using information from sources marked with the current EO 12958 exemption markings (X1 through X8), the "Declassify on" line will be marked with all exemptions that apply to all sources used. For example, if one source cited "X2", another cited "X3" and the third cited "X5", the Declassify on line would read: "Declassify on: X2,3,5". The most recent date will be used on the "Date of Source" line. For example, a derivatively classified document that uses three sources with the latest source dated 10 February 1996, will be marked:

Derived from: Multiple Sources

Declassify on: Sources marked X2,3,5

Date of Source: 10 February 1996

3. When using one or more sources marked with an indefinite declassification from a previous Executive Order (such as OADR) as well as one or more sources marked with the current EO 12958 exemption markings (X1 through X8), the "Declassify on" line will cite the exemption category or exemption categories as well as "source marked OADR". The "Date of Source" line will cite the date of the most recent source. For example, a derivatively classified document that uses the three sources mentioned in subparagraph (2), above, and also uses a source dated 1 September

1995 and marked OADR will be marked:

Derived from: Multiple Sources

Declassify on: Sources marked X2,3,5 and OADR

Date of Source: 10 February 1996

4. The above rules apply to derivatively classified documents when a combination of original classification and derivative sources are used. The term "sources" as used above also includes the classification guides or guidance supplied by the original classifier.

5. With sources having a combination of differing declassification instructions, it is important to determine which is the most restrictive. The most restrictive marking will always be used. This rule applies for all derivative classifications including those in which there is a combination of derivative sources and original classification. A marking that does not provide a definite declassification date will always be considered more restrictive than one with a specific date. For instance, a document that is classified by two sources, one dated 19 August 1994 and marked "OADR" and the other dated 10 December 1995 and marked "Declassify on: 24 May 2004", will be marked: "Declassify on: Source marked "OADR", Date of Source: 19 August 1994". See subportion (3) directly above for an example of a case in which one source is marked OADR and the other is marked with one or more of the exemption categories (X1 through X8) of Executive Order 12958.

#### **4-11. Sources that were created prior to 1976**

Chapter 3 provides the policy for marking information contained in records that will be more than 25 years old on 17 October 2001, and have been determined to have permanent historical value under title 44, USC. In summary, under EO 13142, amendment to EO 12958, section 3.4, information more than 25 years old by 17 October 2001, and that is contained in records that have been determined to have permanent historical value under title 44, USC will be automatically declassified starting on 17 October 2001, unless that information is exempted from declassification. The exemption categories, required markings, and the DA policy for handling this program are discussed in chapter 3 of this regulation. This section is not intended to prescribe the policy for addressing the review of that information. That policy is contained in chapter 3. This section prescribes the policy to follow when material, that will be over 25 years old by 17 October 2001, is used as the source for derivatively classifying a newly created document. Commands will consult AR 25-400-2 and local records managers for advice on what constitutes a file determined to have permanent historical value under Title 44, USC. In creating new documents using the old sources that will be over 25 years on 17 October 2001, it will make a difference whether or not the information has already been reviewed to determine if it is in a record that has been determined to have permanent historical value and whether or not it has been reviewed to determine if it will be declassified or exempted from automatic declassification. There are three possible options:

a. The information is determined to be of permanent historical value under title 44, USC, has been reviewed for continued classification, and qualifies under one or more of the exemptions listed in paragraph 3-6e of this regulation (section 3.4 of EO 12958). If it qualifies for exemption, the exemption category and the future date or event for declassification (if one applies) will be shown on the document, file, or record. When one of these documents is used as a source in classifying a derivatively classified newly created document, use the term shown on the document or record that was applied when the information was reviewed. That term will be "25X" followed by the appropriate exemption category that pertains to information exempted from declassification at 25 years and state the new declassification date or event, if one has been determined. For example, "25X3(31 December 2015)" if the information is exempted because it reveals information that would impair U.S. cryptologic systems and now has been determined to be declassified on 31 December 2015. Sometimes there will only be the exemption category with no date or event listed for declassification. For example, "25X1" if the information would reveal the identity of a human intelligence source.

b. The information is contained in a record that has been determined to have permanent historical value under title 44, USC, has been reviewed, and has been determined to not qualify for exemption. This information will have been marked with a declassification date or event on or before 17 October 2001. This date or event will be used as declassification instructions.

c. The information is either in a record that has been determined to not have permanent historical value under title 44 USC; or is in a record that has been determined to have permanent historical value under title 44 USC but has not yet been reviewed for declassification. This information would be subject to declassification 25 years from the date of its origin. Thus, the date of the source document will be placed, as the following, for declassification instructions: Source marked OADR  
Date of Source(fill in applicable date)

#### **4-12. Warning notices**

In certain circumstances, warning notices will be required if the document contains certain categories of information for which the notice applies. In addition to the notices listed below, other notices may be required by other DA regulations. Unless another regulation or authorized administrative publication prescribes different placement, these notices will be placed on the cover (or first page where there is no cover) of the document.

a. *Restricted Data (RD)* Documents containing RD will be marked: "RESTRICTED DATA" THIS MATERIAL

CONTAINS RESTRICTED DATA AS DEFINED IN THE ATOMIC ENERGY ACT OF 1954. UNAUTHORIZED DISCLOSURE SUBJECT TO ADMINISTRATIVE AND CRIMINAL SANCTIONS.

*b. Formerly Restricted Data (FRD).* Documents containing FRD, but no Restricted Data, will be marked: "FORMERLY RESTRICTED DATA" "Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954."

*c. Critical Nuclear Weapons Design Information (CNWDI).* Messages containing CNWDI will be marked at the beginning of the text as "RD CNWDI." Documents containing CNWDI will be marked: "Critical Nuclear Weapons Design Information DOD Directive 5210.2 applies"

*d. Intelligence Information.* The policy on the control, dissemination, and marking of warning notices concerning intelligence information is contained in appendix D. Placement of these intelligence control markings will follow the same policy as stated in appendix D.

*e. COMSEC Material.* The following marking will be placed on COMSEC documents before release to contractors: "COMSEC Material - Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance."

*f. Reproduction Notices.* Classified information that is subject to dissemination or reproduction limitations will be marked with notices that say, in essence, the following: "Reproduction requires approval of originator or higher DOD authority of the originator". "Further dissemination only as directed by (insert appropriate office or official) or higher DOD authority"

*g. Special Access Programs (SAPs) Documents.* Special Access Programs documents may be identified with the phrase "Special Access Required" and the assigned nickname, codeword, trigraph, or digraph. AR 380-381 contains the Department of the Army policy on marking SAPs material. See appendix I for further information.

*h. DODD 5230.24* requires distribution statements to be placed on technical documents, both classified and unclassified. These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office may, of course, make case-by-case exceptions to distribution limitations imposed by the statements. Distribution statements on technical documents will be marked with notices that say, in essence, the following:

(1) Distribution Statement A — Approved for public release; distribution is unlimited.

(2) Distribution Statement B — Distribution authorized to U.S. Government agencies only; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(3) Distribution Statement C — Distribution authorized to US Government agencies and their contractors; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(4) Distribution Statement D — Distribution authorized to the DOD and US DOD contractors only; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(5) Distribution Statement E — Distribution authorized to DOD Components only; [reason]; [date]. Other requests for this document shall be referred to [controlling DOD office].

(6) Distribution Statement F — Further distribution only as directed by [controlling DOD office] or higher DoD authority; [date].

(7) Distribution Statement X — Distribution authorized to US Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with regulations implementing 10 USC 140c; [date]. Other requests must be referred to [controlling DOD office].

*i. Documents containing information provided by a foreign government.* See section VI of this chapter for complete policy on marking foreign government information in classified DA documents. U.S. classified documents that contain extracts of information provided by a foreign government will be marked with the following warning notice: "FOREIGN GOVERNMENT INFORMATION"

*j. Documents containing information provided by a foreign government or international organization.* See section VII of this chapter for complete policy on marking information provided by a foreign government or international organization. Examples of an international organization are the United Nations (UN) and the North Atlantic Treaty Organization (NATO). The following example pertains to NATO. The same policy applies to any other international organization by replacing the word "NATO" with the appropriate name or abbreviation for that organization. DA classified documents that contain extracts of NATO classified information will bear a marking substantially as follows: "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION"

*k. The following warning notice must appear on all U.S. Government owned or operated automated information systems:*

"THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (INCLUDES INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED, FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST

UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES."

*l.* Other Warning Notices. Subparagraphs a through k above represent the most commonly used warning notices. They do not necessarily represent the only warning notices. There is nothing in this regulation that prohibits other authorized warning notices from being applied to classified documents. Where other regulations authorize and require special warning notices, they may be applied to DA classified documents.

#### **4-13. Obsolete Restrictions and Control Markings**

*a.* The following control markings are obsolete and will not be used, in accordance with the following guidelines:

(1) *WNINTEL* and *NOCONTRACT*. The control markings, Warning Notice - Intelligence Sources or Methods Involved (*WNINTEL*), and NOT RELEASABLE TO CONTRACTORS/CONSULTANTS (abbreviated *NOCONTRACT* or *NC*) were rendered obsolete effective 12 April 1995. No permission of the originator is required to release, in accordance with this directive, material marked *WNINTEL*. Holders of documents prior to 12 April 1995 bearing the *NOCONTRACT* marking should apply the policies and procedures contained in DCID 1/7, section 6.1, for possible release of such documents.

(2) *Remarking*. Remarking of material bearing the *WNINTEL*, or *NOCONTRACT*, control marking is not required; however, holders of material bearing these markings may line through or otherwise remove the marking(s) from documents or other material.

(3) Obsolete markings. Other obsolete markings include: WARNING NOTICE-INTELLIGENCE SOURCES OR METHODS INVOLVED, WARNING NOTICE-SENSITIVE SOURCES AND METHODS INVOLVED, WARNING NOTICE-INTELLIGENCE SOURCES AND METHODS INVOLVED, WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, USIB ONLY, NFIB ONLY.

*b.* Questions with respect to current applications of all control markings authorized by earlier directives on the dissemination and control of intelligence and used on documents issued prior to the effective date of DCID 1/7, 30 June 1998, should be referred to the agency or department originating the intelligence so marked.

#### **4-14. Downgrading instructions**

Downgrading instructions are not required for every classified document, but they must be placed on the face of each document to which they apply. When the original classification authority has determined that a document will be downgraded to a lower classification upon the passage of a date or event, the document will be marked: "Downgrade to SECRET on..." followed by the date or event, and/or "Downgrade to CONFIDENTIAL on..." followed by the date or event. This marking is placed immediately before the "Declassify on" line and is used in addition to, and not as a substitute for, declassification instructions.

#### **4-15. The Modern Army Recordkeeping System**

*a Purpose.* The purpose of Army recordkeeping is to properly manage information, from its creation through final disposition, according to federal laws and Army recordkeeping requirements. AR 25-400-2:

(1) Establishes the Modern Army Recordkeeping System (MARKS) as a portion of the Army Information Resources Management Program (AIRMP).

(2) Furnishes the only legal authority for destroying nonpermanent Army information.

(3) Provides life-cycle management instructions for the systematic identification, maintenance, storage, retirement, and destruction of Army information recorded on any medium (paper, microforms, electronic, or any other).

(4) Ensures that the commander and staff have the information needed to accomplish the mission; that they have it when and where they need it; that they have it in usable format; and that it is created, maintained, used, and disposed of at the least possible cost.

(5) Preserves those records needed to protect the rights and interests of the Army and its members and former members, and those that are of permanent value.

(6) Ensures records related to matters involved in administrative or legal proceedings will be retained until the staff judge advocate or legal adviser authorizes resumption of normal disposition.

(7) Provides for the systematic removal of less active records from office space to low-cost storage space.



*b. Application.* MARKS applies to—

- (1) All unclassified Army records, including For Official Use Only (FOUO) and sensitive, regardless of media.
- (2) All classified Army records through SECRET. Records that are TOP SECRET may be set up under MARKS, or in any manner that will make accountability and control easier. Regardless of the arrangement used, however, the disposition instructions in this regulation, and under MARKS, will be applied to TOP SECRET records.

*c. Principles.*

- (1) Within the MARKS system, records are identified and filed under the number of the primary directive that prescribes those records be created, maintained, and used.
- (2) The file number is the key to MARKS. It identifies the records for filing and retrieval. MARKS numbers are made up by the prescribing directive number followed by an alpha suffix. See section II, appendix F, for the recordkeeping requirements of file titles and dispositions for records created and maintained under the purview of this regulation.

*d. Further guidance.* Further guidance on the management and disposition of files and records can be found in AR 25-400-2.

## **Section II**

### **Marking Special Types of Documents**

#### **4-16. Documents with component parts**

If a classified and/or sensitive document has components likely to be removed and used or maintained separately, each component will be marked as a separate document. Examples of components are annexes, appendices, major parts of a report, or reference charts. If the entire major component is UNCLASSIFIED, it can be marked on its face, top and bottom: "UNCLASSIFIED", and a statement added: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." No further markings are required on this type of component.

#### **4-17. Transmittal documents**

Transmittals are documents that have classified and/or sensitive documents enclosed with or attached to them. An example is a letter with classified enclosures or a document that is used to describe the transmission of classified equipment, documents, or other material. The transmittal document itself may contain information classified and/or sensitive the same or higher than the material transmitted. Often the transmittal document itself is UNCLASSIFIED or classified at a lower level than the material being transmitted or enclosed.

*a.* If the transmittal contains information classified and/or sensitive the same or higher than the documents being transmitted, the transmittal will be marked the same as any other classified and/or sensitive document.

*b.* If the information in the transmittal is UNCLASSIFIED or classified at a lower level than one or more of the documents being transmitted, the transmittal will be marked as follows:

(1) Mark the face of the transmittal conspicuously, top and bottom, in letters larger than the rest of the text, with the highest classification found in any of the enclosed documents being transmitted. For example, an UNCLASSIFIED transmittal that has one SECRET and two CONFIDENTIAL enclosures or attachments will be marked "SECRET".

(2) Mark the face of the transmittal to show its classification status when separated from the material being transmitted. For example, the following or similar statements apply: "UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURES," "UNCLASSIFIED WHEN ATTACHMENT 3 IS REMOVED," "CONFIDENTIAL UPON REMOVAL OF ENCLOSURES," "REGRADED CONFIDENTIAL WHEN SEPARATED FROM ENCLOSURES," etc.

*c.* Any special warning notices that apply to the transmittal or to the documents being transmitted will be placed on the face of the transmittal document. Transmittals that are classified standing alone will be marked the same as other classified documents. UNCLASSIFIED transmittals will not be portion marked. The marking of classification at the top and bottom of interior pages of an UNCLASSIFIED transmittal is not required, but is encouraged.

#### **4-18. Classification by compilation**

When a document is classified and/or sensitive by compilation as discussed in paragraph 2-13, it will be marked as specified in paragraph 4-6d.

#### **4-19. Translations**

Translations of U.S. classified and/or sensitive information into a foreign language, will be marked with the appropriate U.S. classification/sensitivity markings and the foreign language equivalent. Section VIII, of this chapter, contains a list of foreign language classifications. The translations will clearly show the United States as the country of origin.

#### **4-20. Electronically transmitted messages**

This section does not pertain to documents transmitted by facsimile (FAX) transmission. Classified and/or sensitive

## **Chapter 5**

### **Controlled Unclassified Information**

#### **Section I**

#### **For Official Use Only Information**

##### **5-1. General**

a. The requirements of the information security program apply only to information that requires protection in order to prevent damage to the national security and has been classified in accordance with EO 12958 or its predecessors. There are other types of information that require application of controls and protective measures for a variety of reasons. In accordance with DODD 5200.1-R this information is known as Controlled Unclassified Information (CUI). Since classified information and CUI exist side by side in the work environment, often in the same documents, this chapter is provided as an attempt to avoid confusion and promote proper handling. It covers several types of CUI, and provides basic information about the nature of this information and the procedures for identifying and controlling it. In some cases, the chapter refers to other DOD directives that provide more detailed guidance.

b. The types of information covered in this chapter include "For Official Use Only" information, "Sensitive But Unclassified" (formerly "Limited Official Use") information, "DEA Sensitive Information," "DOD Controlled Unclassified Nuclear Information," "Sensitive Information" as defined in the Computer Security Act of 1987, and information contained in technical documents.

##### **5-2. Description**

a. For Official Use Only (FOUO) is a designation that is applied to unclassified information which is exempt from mandatory release to the public under the Freedom of Information Act (FOIA) (see AR 25-55 for more details). The FOIA specifies nine categories of information which can be withheld from release if requested by a member of the public. They are:

- (1) Information which is currently and properly classified.
- (2) Information which pertains solely to the internal rules and practices of the agency. This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document which, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. The "low" profile permits withholding, if there is no public interest in the document, and it would be an administrative burden to process the request.
- (3) Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
- (4) Information, such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis, which, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.
- (5) Intra-agency memoranda which are deliberative in nature; this exemption is appropriate for internal documents which are part of the decision making process and contain subjective evaluations, opinions and recommendations.
- (6) Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
- (7) Records or information compiled for law enforcement purposes that:
  - (a) Could reasonably be expected to interfere with law enforcement proceedings.
  - (b) Would deprive a person of a right to a fair trial or impartial adjudication.
  - (c) Could reasonably be expected to constitute an unwarranted invasion of personal privacy of others.
  - (d) Disclose the identity of a confidential source.
  - (e) Disclose investigative techniques and procedures.
  - (f) Could reasonably be expected to endanger the life or physical safety of any individual.
- (8) Certain records of agencies responsible for supervision of financial institutions.
- (9) Geological and geophysical information concerning wells.
- b. Information which is currently and properly classified can be withheld from mandatory release under the first exemption category (subparagraph (1) above). FOUO is applied to information which is exempt under one of the other eight categories (subparagraphs (2) through (9) above). So, by definition, information must be unclassified in order to be designated FOUO. If an item of information is declassified, it can be designated FOUO if it qualifies under one of those other eight categories. This means that:

- (1) Information cannot be classified and FOUO at the same time; and



(2) Information which is declassified can be designated FOUO, but only if it fits into one of the last eight exemption categories (categories (2) through (9) above).

c. The FOIA provides that, for information to be exempt from mandatory release, it must fit into one of the qualifying categories and there must be a legitimate government purpose served by withholding it. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets this dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records (for example, personnel records) are not normally marked FOUO, but can still qualify for withholding under the FOIA. Only personnel officially appointed as a Release Authority can release Army information.

### **5-3. Marking**

a. Information which has been determined to qualify for FOUO status should be indicated, by markings, when included in documents and similar material. Markings should be applied at the time documents are drafted, whenever possible, to promote proper protection of the information.

b. Wholly unclassified documents and material containing FOUO information will be marked as follows:

(1) Documents will be marked "FOR OFFICIAL USE ONLY," in letters larger than the rest of the text, where practical, at the bottom of the front cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one).

(2) Pages of the document which contain FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom.

(3) Material other than paper documents, for example, slides, computer media, films, etc., will bear markings which alert the holder or viewer that the material contains FOUO information.

(4) FOUO documents and material, transmitted outside the Department of Defense, must bear an expanded marking on the face of the document so that non-DOD holders understand the status of the information. A statement similar to this one should be used: This document contains information Exempt from mandatory disclosure under the FOIA. Exemption(s) (indicate the exemption(s)) apply.

c. Classified documents and material containing FOUO information will be marked as required by chapter 4 of this regulation, with FOUO information identified as follows:

(1) Overall markings on the document will follow the procedures in chapter 4. No special markings are required on the face of the document because it contains FOUO information.

(2) Portions of the document will be marked with their classification as required by chapter 4. If there are unclassified portions which contain FOUO information, they can be marked with "FOUO" in parentheses at the beginning of the portion. Since FOUO information is, by definition, unclassified, the "FOUO" is an acceptable substitute for the normal "U."

(3) Pages of the document which contain classified information will be marked as required by chapter 4 of this regulation. Pages which contain FOUO information but no classified information will be marked "FOR OFFICIAL USE ONLY" at the top and bottom.

d. Transmittal documents which have no classified material attached, but do have FOUO attachments, will be marked with a statement similar to this one: "FOR OFFICIAL USE ONLY ATTACHMENT."

e. Each part of electronically transmitted messages containing FOUO information will be marked appropriately. Unclassified messages containing FOUO information will contain the abbreviation "FOUO" before the beginning of the text.

### **5-4. Access to FOUO information**

FOUO information can be disseminated within DOD components and between officials of Army components and Army contractors, consultants, and grantees, as necessary, in the conduct of official business. FOUO information can also be released to officials in other departments and agencies of the Executive and Judicial Branches in performance of a valid government function. Special restrictions can apply to information covered by the Privacy Act. Release of FOUO information to members of Congress is covered by DODD 5400.4, and to the General Accounting Office by DODD 7650.1.

### **5-5. Protection of FOUO information**

a. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. After working hours, FOUO information can be stored in unlocked containers, desks or cabinets if U.S. Government or U.S. Government-contract building security is provided, or in locked desks, file cabinets, bookcases, or similar items.

b. FOUO documents and material can be transmitted via first class mail, parcel post, or, for bulk shipments, fourth class mail. Electronic transmission of FOUO information by voice, data, facsimile or similar means, should be by approved secure communications systems whenever possible.

c. Record copies of FOUO documents will be disposed of in accordance with AR 25-400-2. Non-record FOUO documents can be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

#### **5-6. Further guidance**

Further guidance on safeguarding personal information is contained in DOD 5400.11-R.

### **Section II**

#### **Sensitive But Unclassified and Limited Official Use Information**

##### **5-7. Description**

Sensitive But Unclassified (SBU) information is information originated within the Department of State which warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act. Prior to 26 January 1995, this information was designated and marked Limited Official Use (LOU). The LOU designation will no longer be used.

##### **5-8. Marking**

The Department of State does not require that SBU information be specifically marked, but does require that holders be made aware of the need for controls. When SBU information is included in DOD documents, the documents will be marked as if the information were FOUO. There is no requirement to remark existing material containing LOU information.

##### **5-9. Access to SBU information**

Within the Department of the Army, the criteria for allowing access to SBU information are the same as those required for FOUO information (see paragraph 5-4).

##### **5-10. Protection of SBU information**

Within the Department of the Army, SBU information will be afforded the same protection as that required for FOUO information (see paragraph 5-5).

### **Section III**

#### **Drug Enforcement Administration Sensitive Information**

##### **5-11. Description**

Drug Enforcement Administration (DEA) sensitive information is unclassified information which is originated by DEA and requires protection against unauthorized disclosure in order to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports. The administrator, and certain other officials, of the DEA have been authorized to designate information as "DEA SENSITIVE". The Department of Defense has agreed to implement protective measures for the following DEA sensitive information in its possession.

- a. Information and material that is investigative in nature.
- b. Information and material to which access is restricted by law.
- c. Information and material which is critical to the operation and mission of the DEA.
- d. Information and material in which the disclosure of such would violate a privileged relationship.

##### **5-12. Marking**

a. Unclassified documents containing DEA sensitive information will be marked "DEA SENSITIVE," in letters larger than the rest of the text, where practical, at the top and bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one).

b. In unclassified documents, each page containing DEA sensitive information will be marked "DEA SENSITIVE" top and bottom. Classified documents containing DEA sensitive information will be marked as required by chapter 4, except that pages containing DEA sensitive information, but no classified information, will be marked "DEA SENSITIVE" top and bottom.

c. Portions of DA documents which contain DEA sensitive information will be marked "(DEA)" at the beginning of the portion. This applies to classified, as well as unclassified documents. If a portion of a classified document contains both classified and DEA sensitive information, the "DEA" marking will be included along with the parenthetical classification marking. For example, a document containing DEA sensitive information along with SECRET information will be marked "(S)(DEA)."

##### **5-13. Access to DEA sensitive information**

Access to DEA sensitive information will be granted only to persons who have a valid need-to-know for the

USC 33) and component records management directives. Non-record DOD UCNI documents can be destroyed by shredding or tearing into pieces and discarding the pieces in regular trash containers.

## **Section V**

### **Sensitive Information (Computer Security Act of 1987)**

#### **5-19. Description**

a. The Computer Security Act of 1987 established requirements for protection of certain information in federal government Automated Information Systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

b. Two aspects of this definition deserve attention. First, the Computer Security Act of 1987 applies only to unclassified information which deserves protection. Second, unlike most other programs for protection of information, the Computer Security Act of 1987 is concerned with protecting the availability and integrity, as well as, the confidentiality of information. Much of the information which fits the Computer Security Act of 1987's definition of "sensitive" falls within the other categories of information discussed in this chapter.

#### **5-20. Marking**

There is no specific marking authorized for the designation of "sensitive" information. If the information fits within one of the other categories of information described in this chapter, the appropriate marking requirements apply.

#### **5-21. Access to sensitive information**

If sensitive information falls within one of the other categories of information described in this chapter, the specific limitations on access for the appropriate category will be applied. If it does not, access to the information will be limited only to those with a valid need for such access in order to perform a legitimate organizational function, as dictated by common sense principles of security management, learned through a proper and thorough security education program.

#### **5-22. Protection of sensitive information**

Information on a DA AIS, which is determined to be "sensitive," within the meaning of the Computer Security Act of 1987, will be provided protection which is:

- a. Determined after thorough consideration of the value and sensitivity of the information and the probable adverse impact of loss of its availability, integrity or confidentiality.
- b. In compliance with applicable DA policy and requirements for security of information within automated systems.
- c. Commensurate with the degree of protection required for the category of information described in this chapter to which it belongs (if any).
- d. Based on sound application of risk management techniques and procedures.

#### **5-23. Further guidance**

Further guidance is found in appendix E of this regulation, AR 380-19, DODD 5200.28, and other related publications.

#### **5-24. Technical documents**

DODD 5230.24 and AR 70-11 require distribution statements to be placed on technical documents no matter if they are classified or unclassified (See figure 5-1). These statements facilitate control, distribution and release of these documents without the need to repeatedly refer questions to the originating activity. The originating office can, of course, make case-by-case exceptions to distribution limitations imposed by the statements.

---

## Distribution Statements for Technical Documents

### Distribution Statement A

Approved for public release; distribution is unlimited.

### Distribution Statement B

Distribution authorized to U.S. Government

Agencies only; *[reason]*; *[date]*.

Other requests for this document will be referred to  
*[controlling DOD office]*.

### Distribution Statement C

Distribution authorized to U.S. Government Agencies  
and their contractors; *[reason]*; *[date]*.

Other requests for this document will be referred to  
*[controlling DOD office]*.

### Distribution Statement D

Distribution authorized to the DoD and U.S. DoD  
contractors only; *[reason]*; *[date]*.

Other requests for this document will be referred to  
The*[controlling DOD office]*.

### Distribution Statement E

Distribution authorized to DoD Components only;  
*[reason]*; *[date]*

Other requests for this document will be referred to  
The*[controlling DOD office]*.

### Distribution Statement F

Further distribution only as directed by *[controlling  
DOD office]* or higher DoD authority; *[date]*

### Distribution Statement X

Distribution authorized to U.S. Government Agencies  
and private individuals or enterprises eligible to obtain  
export-controlled technical data in accordance with  
DoD Directive 5230.24; *[date]*.

Controlling DoD office is *[controlling DOD office]*.

---

Figure 5-1. Distribution Statements for Technical Documents

---

Personnel Office (CPO), to be filed in the individual's Official Personnel File (OPF). The form will be filed on the permanent side of the OPF as an adjunct to the DA Form 873. NDAs for civilian employees transferring from one duty station to another, to include transferring to another U.S. Government agency, will transfer as part of their OPF. The NDA will not be removed from the OPF. If a command receives an NDA executed by a current employee while that employee was assigned to another command or agency, the command official receiving the form will forward the NDA to the applicable local or regional supporting CPO for insertion into the OPF as an adjunct to the DA Form 873. When a civilian employee transfers from one duty station to another, the designated command civilian personnel official will ensure that the Standard Form 75 (Request for Preliminary Employment Data) verifies that a completed NDA is on file. These forms, that are maintained in the individual's official personnel folder, will apply the disposition instructions for the official personnel folder.

*b. Military Personnel.* For military personnel, a copy of the NDA will be kept on file by the command security manager, or other designated command official, for verification that the individual has executed the NDA. Copies of nondisclosure agreements, such as SF 312 or SF 189 or similar forms, signed by military personnel, with access to information that is classified under standards put forth by Executive Orders governing security classification, should be maintained separately from personnel security clearance files. This copy will remain in the command file until the individual transfers or is separated from the U.S. Army. Upon the soldier's arrival at the new duty station, the command security manager will maintain a copy of the original, newly signed NDA on file pending the next transfer. The accepting official will forward the original NDA to the address below, where it will be converted to microfiche and filed with the soldier's official records. Upon notification of transfer, the command security manager, or other designated command official, will send the copy of the NDA to the gaining organization's command security manager either by mail or in the possession of the transferring individual.

(1) Active Army Commissioned and Warrant Officers: Commander, U.S. Total Army Personnel Command, ATTN: TAPC-MSR Alexandria, VA 22332-0400.

(2) Active Army Enlisted Personnel: Commander, U.S. Army Enlisted Records and Evaluation Center, ATTN: PCRE-FS, 8899 East 56th Street, Fort Benjamin Harrison, IN 46249-5301.

(3) Reservists: Commander, U.S. Army Reserve Personnel Center, ATTN: DARP-PRD-MP, 9700 Page Avenue, St. Louis, MO 63132-5200. When a cleared Individual Ready Reserve (IRR) member is ordered to active duty for training that will involve access to classified information and previous execution of the NDA cannot be verified, an NDA will be completed at the training site and the original forwarded to the U.S. Army Reserve Personnel Center.

(4) National Guard Commissioned and Warrant Officers: Army National Guard Personnel Division, ATTN: NGB-ARD-C, 111 South George Mason Drive, Arlington, VA 22204-1382.

(5) For National Guard enlisted soldiers: Forward to the soldier's State Adjutant General, ATTN: POMSO.

*c. Department of the Army Consultants and Other Non-U.S. Government Personnel.* If a consultant to the Department of the Army is hired under Civil Service procedures, as opposed to contracting with a company for consultant services, the NDA will be executed and filed with the DA Form 873. If the consultant's OPF is not retired, the command is obligated to retain the NDA for the required 50-year retention period. Consultant NDAs cannot be used by or transferred to another activity. They only authorize access to classified information under a specific agreement and an access termination form must be executed when the agreement has ceased or when classified access is no longer required, whichever occurs first. In special situations where non-U.S. Government uncleared personnel have been granted classified access to specific information in accordance with the policy established in AR 380-67, the NDA will be attached to the exception to policy memorandum or other appropriate written authorization which authorized the individual's access to classified information and will be retained in the command's files for 50 years.

#### **6-4. Refusal to execute the NDA**

If a person refuses to sign the NDA, the individual will be advised of the applicable portions of the NDA, SF 312. The individual will be given five calendar days to reconsider and will not be permitted access to classified information during that time. At the end of the five-day period, the individual will again be requested to sign the NDA. If at that point the individual still refuses to sign the NDA, their classified access, if it had been previously granted, will be formally suspended, the individual will not be permitted any access to classified information, the Department of the Army's Central Clearance Facility will be notified concerning clearance revocation or denial action, and the matter will be reported as required by AR 380-67.

#### **6-5. Debriefing and termination of classified access**

*a.* Classified information is not the personal possession of any DA personnel, regardless of rank, title, or position. Classified information will not be removed to nonofficial or unapproved locations, such as personal residences, upon the termination of employment or military service of any person, including the custodian of that material.

*b.* All DA personnel who are retiring, resigning, being discharged, or will no longer have access to classified information, will out-process through the command security manager's office or other designated command office. During this out-processing the individual will be informed that security clearance and access to classified information has terminated and that the individual still has an obligation to protect any knowledge they have of classified information. DA personnel will sign a debriefing statement during out-processing. The debriefing statement will either

be the NDA Security Debriefing Acknowledgement section of the SF 312, or DA Form 2962 (Security Termination Statement). The debriefing, as a minimum, will consist of informing the individual of the continuing obligation to protect classified information accessed, the admonition that discussion or other revelation of classified information to unauthorized persons is prohibited, provide instructions for reporting any unauthorized attempt to gain access to classified information, advise the individual of the prohibition against retaining classified material when leaving the command, and remind the individual of the potential civil and criminal penalties for failure to fulfill these continuing responsibilities. The same procedures will be followed for DA personnel still employed and still in service whose security clearance has been withdrawn, denied (after interim access was granted), or revoked either for cause or for administrative reasons due to lack of need for future access to classified information. In these cases both civilian and military DA personnel will execute the debriefing statement.

c. Unless exempted by the senior security official at the MACOM, security out-processing is required for all cleared personnel transferring to another DA command or to a Federal Government agency. Transfers will not require the execution of the type of debriefing statement described in subparagraph b, above. This does not preclude the command from requesting the transferring individual sign or initial a form or statement indicating, in substance, that the individual has been advised of the continuing responsibility to protect classified information and/or has completed the security out-processing. Personnel transferring will be briefed on the responsibilities stated in subparagraph b, above. Additionally, personnel transferring will be advised that classified information previously created, or in the custody of, the individual, including that gained while attending training or conferences, does not belong to the individual and does not transfer to the gaining command without appropriate approval by both the gaining and losing commands. Such approval will be based upon the losing command's assessment of the need-to-know for the information by the gaining command. Out-processing can also be used as a means to ensure that the appropriate command security officials are aware of the departure of personnel to ensure combinations and passwords are changed, keys are returned, accountable documents and property are under new custody, etc. Where out-processing is not required for transfers, the command will establish procedures to ensure that the command security manager is advised of such transfers.

d. For all DA military personnel, retiring, resigning, or separating from military service, the DA Form 2962, or the termination portion of the NDA, will be executed and maintained on file by the command security manager, or other designated command official, at the soldier's last duty station, for a period of two years, in accordance with AR 25-400-2.

e. All Army civilian personnel who are retiring or resigning from government service, must out-process through the activity's security office. The security official will debrief the civilian employee about the continuing obligation to protect the classified information accessed during government service. The civilian employee should sign a DA Form 2962 or the NDA Debriefing Acknowledgement, which will be retained by the activity. Signing the NDA Debriefing Acknowledgement is the individual's option upon final separation from the government service, however, the individual will be informed that security clearance and access to classified information has terminated and that the individual still has a legal obligation to protect classified information. The original NDA, for civilian employees, who retire or resign from government service, will remain in the employee's OPF and will be retired as part of the OPF. The NDA (SF 189 or SF 312) for civilian employees who retired or resigned prior to 1993 and are currently filed in an inactive file will be forwarded to: National Personnel Records Center, Civilian Personnel Records, 111 Winnebago Street, St. Louis, MO 63118.

f. Refusal to sign the DA Form 2962 or the termination portion of the NDA, SF 312, will be considered a lack of personal commitment to protect classified information. Personnel who refuse to sign a termination statement will not be granted further access to classified information and their security clearance may be revoked or denied in accordance with AR 380-67.

#### **6-6. Communication and cooperation between command officials**

Commanders will establish policy and procedures to ensure that other command officials and personnel advise the command security manager of any information affecting an individual's access to classified information. Personnel officials will make sure that transfer and recruitment documents, including vacancy announcements, indicate if a security clearance is required for the position.

#### **6-7. Access to restricted data, formerly restricted data, and critical nuclear weapons design information**

a. Access to RD (less CNWDI) and FRD by DA personnel, at Army facilities, will be under the same conditions as for all other classified information, based on the appropriate security clearance and access, need-to-know for the information, and in accordance with DODD 5210.2. See paragraph 6-17 for the requirement for DA certification to access classified information, including RD and FRD, held by Department of Energy (DOE) personnel and for classified visits to DOE certified facilities. Because of the sensitivity of nuclear information, the need-to-know criteria will be strictly enforced for all access to RD and FRD information.

b. Critical Nuclear Weapons Design Information (CNWDI) is a category of SECRET and TOP SECRET restricted data. Access to and dissemination of CNWDI is of particular concern to national security. Access to CNWDI will be limited to U.S. citizens with final TOP SECRET or SECRET, as appropriate to the information being accessed,

When effectively implemented the EEP provides visibility and emphasis to the command security program. Its use is a command option. The Two Person Integrity (TPI) Program is, effective by this regulation, no longer a Department of the Army-wide requirement. Personnel are reminded that the unauthorized disclosure of TOP SECRET information can result in exceptionally grave damage to national security. TPI is a tool that can be used to better protect this high level of classification and should be considered for inclusion in command security programs. Its use is also a command option. Two persons are required, however, for the destruction of TOP SECRET material as stated in paragraph 6-29, and may be required for SAPs (see AR 380-381).

## **Chapter 7**

### **Storage and Physical Security Standards**

#### **Section I**

##### **General**

##### **7-1. Policy**

Classified information will be secured under conditions adequate to prevent access by unauthorized persons and meeting the minimum standards specified in this regulation. An assessment of the threat to the material, the location of the command, and the sensitivity of the information, will be considered when determining if the minimum requirements of this Chapter require enhancement, as determined by the local command. Based upon an assessment of the threat, the command will institute appropriate security measures designed to make unauthorized access so difficult that an intruder will hesitate to attempt to try to gain access or enhance the likelihood of discovery and apprehension if an unauthorized access is attempted.

##### **7-2. Physical security policy**

a. Physical security is intended to be built upon a system of defense, or security in depth, to provide accumulated delay time. AR 190-13, AR 190-16, and Field Manual (FM) 19-30, provide additional information on the principals of physical security. For technical assistance concerning classified material physical security storage standards, commands can contact the Army Intelligence Materiel Activity (IMA), Intelligence Materiel Management Center, Fort George G. Meade, MD 20755-5315.

b. AR 190-13 prescribes minimum uniform standards and procedures in the use of security identification cards and badges to control personnel movement into, and movement within, restricted areas. These standards and procedures are established to safeguard facilities against espionage, sabotage, damage, and theft. Security identification cards and badges may be used to control access to installations and activities. They will be used in addition to other required identification cards to military personnel, civilian DOD and contractor employees, and visitors entering installations, activities, or restricted areas, as determined by the commander concerned.

#### **Section II**

##### **Storage Standards**

##### **7-3. Standards for storage equipment**

General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for the storage and protection of classified information.

##### **7-4. Storage of classified information**

a. Classified information that is not under the personal control and observation of an authorized person, is to be guarded or stored in a locked security container, vault, room, or area, pursuant to the level of classification and this regulation by one or more of the following methods:

(1) TOP SECRET information will be stored as identified below:

(a) A GSA-approved security container with one of the following supplemental controls:

1. The location that houses the security container will be subject to continuous protection by cleared guard or duty personnel.

2. Cleared guard or duty personnel will inspect the security container once every two hours, but not in a way that indicates a pattern.

3. An Intrusion Detection System (IDS), meeting the requirements of section III of this Chapter, with personnel responding to the alarm, arriving within 15 minutes of the alarm annunciation.

4. Security-in-depth when the GSA-approved container is equipped with a lock meeting Federal Specification FF-L-2740A. See appendix J for a definition of security-in-depth.

(b) A vault, modular vault, or security room constructed in accordance with section III of this Chapter, and equipped



with an IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation if the area is covered by security-in-depth, or a 5 minute alarm response time if it is not. Other rooms that were approved under former policy for the storage of TOP SECRET in the U.S. can continue to be used.

(c) New purchases of combination locks for GSA-approved security containers, vault doors and secure rooms will conform to Federal Specification FF-L-2740A. Existing, non-FF-L-2740A mechanical combination locks will not be repaired. If they should fail, they will be replaced with locks meeting FF-L-2740A. See section IV for information on retrofitting locks (replacing locks with those meeting Federal Specification FF-L-2740A) on existing containers where the lock is not in need of repair.

(d) Under field conditions, during military operations, commanders can prescribe the measures deemed adequate to meet the storage standard contained in subparagraphs 1 and 2 above.

(2) SECRET information will be stored—

(a) In the same manner as prescribed for TOP SECRET.

(b) In a GSA-approved security container or vault without supplemental controls.

(c) In secure rooms that were approved for the storage of SECRET or CONFIDENTIAL information by the 28 February 1988 edition of this regulation, provided that the approval for storage occurred prior to 1 October 1995.

(d) Until 1 October 2002, in a non-GSA-approved container having a built-in combination lock, or in a non-GSA-approved container secured with a rigid metal lock-bar and a GSA-approved padlock with one or more of the following supplemental controls.

1. The location that houses the container is subject to continuous protection by cleared guard or duty personnel.

2. Cleared guard or duty personnel will inspect the security container once every four hours, using random times.

3. An IDS with the personnel responding to the alarm arriving within 30 minutes of the alarm. In order to reduce the risk of the lock being swapped while the container is opened, the padlock will be secured to the hasp in the locked position, or the padlock will be locked and placed inside the cabinet. Commands are encouraged to replace the non-GSA-approved cabinets with GSA-approved security containers as soon as feasible, prior to the mandatory replacement date of 1 October 2002. New lock-bar cabinets will not be fabricated from either existing or new containers, nor will any existing lock-bar container, that was not previously used for the protection of classified information, be put into use for that purpose.

(3) CONFIDENTIAL information will be stored in the same manner as prescribed for TOP SECRET and SECRET information except that supplemental controls are not required. Where lock-bar cabinets are used, in order to reduce the risk of the lock being swapped while the container is open, the padlock will be secured to the hasp in the locked position, or the padlock will be locked and placed inside the cabinet. Commands are encouraged to replace the non-GSA-approved cabinets with GSA-approved security containers as soon as feasible prior to the mandatory replacement date of 1 October 2002. New lock-bar cabinets will not be fabricated from either existing or new containers, nor will any existing lock-bar container, that was not previously used for the protection of classified information, be put into use for that purpose.

b. *Specialized security equipment.*

(1) GSA-approved field safes and special purpose, one and two drawer, light-weight, security containers, approved by the GSA, are used primarily for storage of classified information in the field and in military platforms, and will be used only for those or similar purposes. Such containers will be securely fastened to the structure or under sufficient surveillance to prevent their theft or compromise.

(2) GSA-approved map and plan files are available for storage of odd-sized items such as computer media, maps, charts, and classified equipment.

(3) GSA-approved modular vaults, meeting Federal Specification AA-V-2737, can be used to store classified information as an alternative to vault requirements described in section III of this Chapter.

c. *Replacement of combination locks* The mission and location of the command, the classification level and sensitivity of the information, and the overall security posture of the activity, are factors used in determining the priority for replacement of existing combination locks. All system components and supplemental security measures, including electronic security systems (e.g., intrusion detection systems, automated entry control subsystems, and video assessment subsystems), and level of operations, must be evaluated by the command when determining the priority for replacement of security equipment. Section IV of this Chapter provides a matrix illustrating a prioritization scheme for the replacement of existing combination locks on GSA-approved security containers and vault doors, and can be used as a guide for this purpose. The prioritization scheme can be tailored to specific environments and sensitivity of information stored. Priority 1 requires immediate replacement. Replacement is generally considered to be accomplished when the equipment is obtained and installed within the framework of the command budget constraints, but in no event will exceed two years from the effective date of this regulation.

d. *Storage areas.* Storage areas, for bulky material containing SECRET or CONFIDENTIAL information, can have access openings secured by GSA-approved, changeable, combination padlocks (Federal Specification FF-P-110 series) or high security, key-operated padlocks (Military Specification MIL-P-43607). Other security measures are required, in accordance with paragraph 7-4a(1), above, for TOP SECRET material, and are strongly recommended for all other levels of classified material.



(1) Commands will establish administrative procedures for the control and accountability of keys and locks whenever key-operated, high-security padlocks are utilized. The level of protection provided such keys will be equivalent to that afforded the classified information being protected by the padlock. As a minimum, the following procedures will be implemented.

(a) A key and lock custodian will be appointed in writing to ensure proper custody and handling of keys and locks.

(b) A key and lock control register will be maintained to identify keys for each lock and their current location and custody.

(c) Keys and locks will be audited at least quarterly.

(d) Keys will be inventoried with each change of custodian. Keys will not be removed from the premises.

(e) Keys and spare locks will be protected in a security container or other secure container.

(f) In order to reduce the risk of the padlock being swapped while the container is opened, the padlock and the key will be either placed in the security container, or the padlock will be locked to the hasp and the key either personally retained, retained at a central location, or placed inside the unlocked container.

(g) Since there is a lesser degree of risk of compromise with key operated locks, they will be changed or rotated at a minimum of once every two years, and will be immediately replaced upon loss or compromise of their keys.

(2) Section 1386 of Title 18, United States Code, makes unauthorized possession of keys, key-blanks, key-ways or locks adopted by any part of the Department of Defense for use in the protection of conventional arms, ammunition, or explosives, special weapons, and classified equipment, a criminal offense punishable by fine or imprisonment for up to 10 years, or both.

#### **7-5. Procurement of New Storage Equipment**

a. New security storage equipment will be procured from those items listed on the GSA Federal Supply Schedule. Exceptions can be made by the MACOM commander, will be fully justified, and will be reported to DAMI-CH, who must notify the Office of the Secretary of Defense (ASD(C31)) of the details of the exception.

b. As stated in paragraph 7-4a(3) above, new lock-bar containers used to store classified material will not be fabricated from either existing or new cabinets, and existing lock-bar containers will be phased out and no longer authorized for use after 1 October 2002.

c. Nothing in this Chapter will be construed to modify existing federal supply class management assignments made under DODD 5030.47.

#### **7-6. Residential storage**

Classified information will not be stored in a personal residence, on or off a military installation. Classified information will not be stored in any location outside an approved location at a U.S. Government or cleared contractor facility. Exceptions are:

a. In extreme and exceptional situations, a MACOM commander, or the Administrative Assistant to the Secretary of the Army for HQDA activities, can approve the temporary storage of SECRET and CONFIDENTIAL material only, in a personal residence, either on or off a military installation, or in another location that is not a U.S. Government or cleared contractor facility. This authority will not be further delegated. A validated operational requirement must exist for consideration of such requests and requests will not be approved for personal convenience. Authorization for such temporary storage must be in writing and will include written procedures for the protection of the information. The material will be stored in a GSA-approved security container and protected with an intrusion detection (alarm) system (IDS). Other methods of supplemental control can be used in place of an IDS, where the other methods provide substantially the same assurance of protection. Physical security standards, beyond the requirement for storage in a GSA-approved security container protected with an IDS, will be determined by the approving official.

b. The Secretary of the Army is the only DA official that can authorize the removal of TOP SECRET information and/or material from designated work areas for temporary storage outside a government or cleared contractor facility, to include the storage at a personal residence on a government facility. MACOM commanders can authorize the removal SECRET, and below, information and/or material from designated work areas for temporary storage outside a government or cleared contractor facility, to include the storage at a personal residence on a government facility. Where such approval is granted, to temporarily store classified information and/or material outside a designated work area at a government or cleared contractor facility, a GSA-approved security container will be furnished for storage. The container will be protected by an (IDS) as prescribed in section III of this Chapter, and written procedures addressing the appropriate protection of the information will be provided to the holder of the material. Other methods of supplemental control can be used in place of an IDS where the other methods provide the same assurance of protection. As a minimum, the written procedures concerning the storage of any level of classified information, will require the material to be under personal control, of the authorized individual, at all times when it is not secured in a GSA-approved security container. Also included will be the identification and signature receipt of the material temporarily stored, the reconciliation of the material upon its return, and the requirement that the material be returned as soon as possible after the operational requirement has ended. All authorizations, irrespective of classification level of material involved, will specify a specific expiration date.

## **Chapter 8**

### **Transmission and Transportation**

#### **Section I**

#### **Methods of Transmission and Transportation**

##### **8-1. Policy**

Classified information will be transmitted and transported only as specified in this Chapter. COMSEC information will be transmitted in accordance with AR 380-40. Special Access Programs material will be transmitted and transported in accordance with appendix I of this regulation, AR 380-381, and applicable SAPs procedure guides. Commands will establish local procedures to meet the minimum requirements to minimize risk of compromise while permitting use of the most effective transmission or transportation means. External, street side, collection boxes, for instance, U.S. Mail boxes, will not be used for the dispatch of classified information. Commands will develop procedures to protect incoming mail, bulk shipments, and items delivered by messenger, until a determination is made whether classified information is contained therein. Screening points will be established to limit access of classified information to only cleared personnel.

##### **8-2. TOP SECRET Information**

TOP SECRET information will be transmitted only by:

- a. A cryptographic system authorized by the Director, NSA, or a protected distribution system designed and installed to meet approved NSA standards. This applies to voice, data, message, and facsimile transmissions.
- b. The Defense Courier Service (DCS) (see DODD 5200.33-R).
- c. Authorized command courier or messenger services.
- d. The Department of State Diplomatic Courier Service.
- e. Cleared U.S. military personnel and U.S. Government civilian employees, traveling by surface transportation, or traveling on a conveyance owned, controlled, or chartered by the U.S. Government or DOD contractors.
- f. Cleared U.S. military personnel and U.S. Government civilian employees on scheduled commercial passenger aircraft.
- g. Cleared DOD contractor employees within and between the United States and its territories, when the transmission has been authorized, in writing, by the appropriate Cognizant Security Agency (CSA), or a designated representative. For DA contractors, the CSA is generally the Defense Security Service (DSS).

##### **8-3. SECRET information**

SECRET information can be transmitted by:

- a. Any of the means approved for the transmission of TOP SECRET information.
- b. U.S. Postal Service registered mail, within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico.
- c. U.S. Postal Service express mail, within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico. The "Waiver of Signature and Indemnity" block on the U.S. Postal Service express mail label 11-B, will not be executed under any circumstances. The use of external, street side, express mail collection boxes is prohibited.
- d. U.S. Postal Service registered mail, through Army, Navy, or Air Force Postal Service facilities, for instance, APO/FPO, outside the United States and its territories, so that the information does not, at any time, pass out of U.S. citizen control, and does not pass through a foreign postal system or any foreign inspection.
- e. United States Postal Service and Canadian registered mail, with registered mail receipt between U.S. Government and Canadian Government installations in the U.S. and Canada.
- f. As an exception, in urgent situations requiring next-day delivery, an overnight or next-day delivery service, that is a current holder of a GSA contract for overnight delivery of material for the Executive Branch, provided that the delivery service is U.S. owned and operated and provides automated in-transit tracking of the material. These companies are not required to be cleared and generally are to be considered uncleared. Their employees are not cleared and are not required to be U.S. citizens, and the companies are not required to meet the storage requirements contained in this regulation. For the purpose of this section of the regulation, an urgent situation exists when the classified material must be received by the next day, there is no other authorized means to make the delivery, excluding the

handcarrying by authorized personnel, the delivery company assures delivery by the required date, and the transmission complies with the provision of Title 39, U.S. Code (USC), section 320.6, Postal Services, as amended. The sender will comply with the requirement contained in paragraph 8-10, to address the package to the command or activity, and not address it to an individual. Since delivery services usually require the building number and name of recipient, the sender will contact the recipient to ensure that an authorized and appropriately cleared person will be available to sign for the material, and they will verify the authorized address to make sure that it is displayed correctly on the package label. Unless it is not possible, for example, if the material is needed on a weekend and the mailroom is not in operation then, the package label will be addressed to a supporting mailroom. The release signature block on the receipt label will not be executed under any circumstances. Executing the release signature block, ensures that someone, but not necessarily the addressee, if the addressee is unavailable when the package is delivered, signs for the package. These precautions are required because uncleared, commercial overnight delivery services can deliver the package directly to the person named, and building identified, on the label, or to whomever signs for the material, if the addressee is unavailable when the material is delivered. U.S. Postal Service mail is delivered or picked-up by a centralized command mailroom where personnel who open mail are cleared and the material is properly safeguarded until opened. The use of external, street side, commercial delivery service collection boxes is prohibited. Note: In many situations, the United States Postal Service express mail can meet the next day delivery standards and should be used, as noted in subparagraph c, above.

g. Carriers authorized to transport SECRET information by way of a Protective Security Service (PSS) under the National Industrial Security Program (NISP). This method is authorized only within the United States boundaries when other methods are impractical.

h. Appropriately cleared contractor employees, provided that the transmission meets the requirements specified in DODD 5220.22-R and DODD 5220.22-M (NISPOM).

i. U.S. Government and U.S. Government contract vehicles, including aircraft, ships of the U.S. Navy, civil service-operated U.S. Navy ships, and ships of United States registry. Appropriately cleared operators of vehicles, officers of ships, or pilots of aircraft, who are U.S. citizens, may be designated as escorts, provided the control of the carrier is maintained on a 24-hour basis. The escort will protect the shipment at all times, through personal observation or authorized storage, to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible, to any unauthorized persons, or in a specialized secure, safe-like container. The escort will, if possible, observe the loading of the shipment.

#### **8-4. CONFIDENTIAL information**

CONFIDENTIAL information may be transmitted by:

a. Means approved for the transmission of SECRET information. However, U.S. Postal Service registered mail will be used for CONFIDENTIAL material only as indicated below:

(1) NATO CONFIDENTIAL information. If NATO CONFIDENTIAL material is sent between U.S. Government activities, within the Continental United States, its territories, and the District of Columbia, it can be sent by first class mail. The caveat, "POSTMASTER: RETURN SERVICE REQUESTED" will be affixed to the outer wrapper.

(2) Other CONFIDENTIAL material sent to and from FPO or APO addressees, located outside the U.S. and its territories.

(3) Other CONFIDENTIAL material when the originator is uncertain that the addressee's location is within U.S. boundaries or knows the addressee's location is outside U.S. boundaries.

b. United States Postal Service certified mail (or registered mail, if required above) for material addressed to DOD contractors or non-DOD agencies.

c. United States Postal Service first class mail between DOD component locations anywhere in the U.S., its territories, and the District of Columbia. The use of external, street side, postal collection mailboxes is prohibited. The outer envelope or wrappers will be endorsed, where possible, in letters larger than the text on the address of the envelope: "POSTMASTER: RETURN SERVICE REQUESTED."

d. Within United States boundaries, commercial carriers that provide a Constant Surveillance Service (CSS).

e. In the custody of commanders or masters of ships of United States registry, who are United States citizens. CONFIDENTIAL information shipped on ships of U.S. registry, cannot pass out of United States control. The commanders or masters must sign a receipt for the material and agree to:

(1) Deny access to the CONFIDENTIAL material by unauthorized persons, including customs inspectors, with the understanding that CONFIDENTIAL cargo, that would be subject to customs inspection, will not be unloaded.

(2) Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

transmittal letter or form, this can be accomplished by inserting an opaque sheet or cardboard sheet on top of the classified text in the inner envelope.

#### **8-10. Addressing**

a. The outer envelope or container for classified material will be addressed to an official government activity or to a DOD contractor with a facility clearance and appropriate storage capability. It will show the complete return address of the sender. The outer envelope will not be addressed to an individual. Office codes or phrases such as "Attention: Research Department" may be used.

b. The inner envelope or container will show the address of the receiving activity, the address of the sender, the highest classification of the contents, including, where appropriate, any special markings such as "RESTRICTED DATA" or "NATO," and any other special instructions. The inner envelope may have an "attention line" with a person's name.

c. The outer envelope or single container will not bear a classification marking or any other unusual marks that might invite special attention to the fact that the contents are classified.

d. Classified information intended only for U.S. elements of international staffs or other organizations, must be addressed specifically to those elements.

#### **8-11. Mail channels with the Department of Energy**

Other federal government agencies can require special certification or special procedures before forwarding classified information to another agency. Where that is the case, DA commands will comply with the requirements of those agencies. Specifically, the Department of Energy (DOE) requires that a "mail channel" be established prior to the transmission of certain classified information from a DOE facility to another activity. The mail channel, or material channel for transmission of material other than mail, will be certified by a designated DA certification official, will be made on DOE Form 5631.20 and will include the certified classified mailing address. The certification official will be one of the officials authorized to sign DOE Form 5631.20. See paragraph 6-17, of this regulation, for policy on personnel authorized to sign the DOE Form 5631.20. The DOE Form 5631.20 replaced DOE Form DP-277. It is recommended that the DOE facility that holds the material be contacted for the proper address and information to be completed on the form. Unless notified to the contrary by the DOE facility, the mail or material channel may not exceed one year, subject to renewal of the form.

### **Section IV**

#### **Escort or Handcarrying of Classified Material**

#### **8-12. General provisions**

a. Appropriately cleared personnel may be authorized to escort or handcarry classified material between locations when other means of transmission or transportation cannot be used. Handcarrying of classified material will be limited to situations of absolute necessity and will be carried out to make sure it does not pose an unacceptable risk to the information. Generally, two-way handcarrying, carrying the material both to and from the destination, is not authorized unless specific justification has been provided and both situations involving the handcarrying meet the requirements stated in this section. Handcarrying will be authorized only when:

(1) The information is not available at the destination and is required by operational necessity or a contractual requirement.

(2) The information cannot be sent by a secure facsimile transmission or by other secure means, for example, U.S. Postal Service express mail.

(3) The handcarry has been authorized by the appropriate official. For handcarrying within and between the United States, its territories, and Canada, the authorizing official will be determined by the commander, subject to MACOM approval. For all other areas, approval is at the MACOM level and can be further delegated in writing by the MACOM. Where delegated, the MACOM will exercise oversight, during inspections and/or assistance visits, by requiring copies of approvals, or by other means, to ensure the requirements of this section are met.

(4) The handcarry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the information will remain in the custody and physical control of the U.S. escort at all times.

(5) Arrangements have been made for secure storage during overnight stops and similar periods. The material will not be kept in hotels, personal residences, vehicles, or any other unapproved storage location.

(6) A receipt for the material, for all classification levels, is obtained from an appropriate official at the destination and the receipt is returned to the appropriate official at the traveler's command.

b. Many of the principles contained in paragraph 8-14, of this regulation, apply to all situations involving the handcarrying of classified information and are not restricted to those situations involving classified material handcarried outside the United States. Commands will consider the principles stated in paragraph 8-13 in developing command

procedures concerning the handcarrying of classified material and incorporate those that are deemed applicable to the handcarrying of classified material within the United States.

#### **8-13. Documentation**

a. Responsible officials will provide a written statement to all individuals escorting or carrying classified material authorizing such transmission.

b. The DD Form 2501 (Courier Authorization Card) may be used to identify appropriately cleared DA personnel who have been approved to handcarry classified material in accordance with the following, except that in the case of travel aboard commercial aircraft, the provisions of paragraph 8-15 of this regulation apply:

- (1) The individual has a recurrent need to handcarry classified information;
- (2) The form is signed by an appropriate official in the individual's servicing security office;
- (3) Stocks of the form are controlled to preclude unauthorized use.
- (4) The form is issued for no more than two years at a time. The requirement for authorization to handcarry will be reevaluated and/or reevaluated on at least an biennial basis, and a new form issued, if appropriate.
- (5) The use of the DD Form 2501 for identification and/or verification of authorization to handcarry Sensitive Compartmented Information or Special Access Programs information, will be in accordance with policies and procedures, established by the official having security responsibility for such information or programs.

#### **8-14. Security requirements for temporary duty travel outside the United States**

a. As stated above, the handcarrying of classified information is not a routine method of transmission and will only be approved when fully justified. Handcarrying classified material outside the United States subjects the information to increased risk. When classified material is handcarried, for delivery to a foreign government representative, or when classified information is discussed with, or otherwise disclosed to, foreign national personnel, the requirements of AR 380-10 will be strictly followed.

b. The DOD requires that a request for travel outside the United States contain a written statement by the traveler that classified information will or will not, as applicable, be disclosed during the trip. If the foreign disclosure of classified information is involved, there will be an additional written statement that disclosure authorization has been obtained in accordance with DODD 5230.11. For DA commands, AR 380-10 applies. The statement also will specify whether authorization has been obtained to carry classified material, in compliance with the provisions of this regulation.

c. If the traveler has been authorized to carry classified material, a copy of the written authorization will accompany the justification for the temporary duty travel (TDY). This authorization, the courier orders, will be provided by the traveler's Special Security Officer (SSO) or Command Security Manager (CSM). They will be kept in a secure place and will not be presented unless circumstances dictate.

d. Because of Operations Security (OPSEC) concerns, Block 16 of DD Form 1610 (Request and Authorization for TDY Travel of DOD Personnel) will not contain statements that identify the traveler as carrying classified information.

e. Travelers who are authorized to carry classified material on international flights, or by surface conveyance if crossing international borders, must have courier orders. The DD Form 2501 is not a valid form of courier authorization for travel overseas. A memorandum on command letterhead is required and will, as a minimum, provide the information specified in subparagraph (11), below. Travelers will be informed of, and acknowledge, their security responsibilities. The latter requirement may be satisfied by a briefing or by requiring the traveler to read written instructions that, as a minimum, contain the information listed below.

- (1) The traveler is liable and responsible for the material being escorted.
- (2) Throughout the journey, the classified material will stay in the personal possession of the traveler, except when it is in authorized storage.
- (3) The material will not be opened en route except in the circumstances described in subparagraph (9), below.
- (4) The classified material is not to be discussed or disclosed in any public place.
- (5) The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies, or cleared contractor facilities will be used. Classified material will not be stored in vehicles, hotel rooms or safes, personal residences, or any other unauthorized storage facility or location.
- (6) The traveler will not deviate from the authorized travel schedule, unless such deviation is beyond the traveler's control, such as cancellation of a flight. The traveler will immediately notify their command of any delays.
- (7) In cases of emergency, the traveler will take appropriate measures to protect the classified material, and will notify their command as soon as possible.
- (8) The traveler is responsible for ensuring that personal travel documentation, such as passport, courier authorization, and medical documents, etc., are complete, valid, and current.

(9) There is no assurance of immunity from search by the customs, police, and/or immigration officials of the various countries whose border the traveler may be crossing. Therefore, should such officials inquire into the contents of the consignment, the traveler will present the courier orders and ask to speak to the senior customs, police and/or immigration official. This action should normally suffice to pass the material through unopened. However, if the senior

)
)
)
)
)
)
)
)
)

 $\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Enclosure 3**

3 August 2012

**FOR OFFICIAL USE ONLY**

Army Regulation 530-1

Operations and Signal Security

# **Operations Security (OPSEC)**

**Distribution Restriction Statement.**

This publication contains technical or operational information that is for official Government use only. Distribution is limited to U.S. Government agencies and their contractors. Requests from outside U.S. Government agencies for release of this publication under the Freedom of Information Act or the Foreign Military Sales Program must be made to HQDA G-3/5/7 (DAMO-ODI), 3200 ARMY PENTAGON, WASHINGTON, DC 20310.

**Destruction Notice.**

Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Headquarters  
Department of the Army  
Washington, DC  
19 April 2007

**FOR OFFICIAL USE ONLY**

## Chapter 1 Introduction

### 1-1. Purpose

This regulation prescribes policy and procedures for operations security (OPSEC) in the Army.

### 1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

### 1-3. Explanation of Abbreviations and Special Terms

Abbreviations and special terms used in this regulation are explained in the glossary.

### 1-4. Responsibilities

Responsibilities are listed in chapter two. Responsibilities referring to commanders and similar terms are equally applicable to equivalent management and supervision positions in organizations that do not employ a traditional military command structure.

### 1-5. Definitions

#### *a. Operations security (OPSEC).*

(1) As defined in DOD Directive (DODD) 5205.02, OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- (a) Identify those actions that can be observed by adversary intelligence systems.
- (b) Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- (c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

(2) Operations security protects critical information from adversary observation and collection in ways that traditional security programs cannot. While these programs such as information security protect classified information, they cannot prevent all indicators of critical information, especially unclassified indicators, from being revealed.

(3) In concise terms, the OPSEC process identifies the critical information of military plans, operations, and supporting activities and the indicators that can reveal it, and then develops measures to eliminate, reduce, or conceal those indicators.

#### *b. Critical information.*

(1) Critical information is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States.

(2) Critical information consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment.

(3) Critical information is information that is vital to a mission that if an adversary obtains it, correctly analyzes it, and acts upon it, the compromise of this information could prevent or seriously degrade mission success.

(4) Critical information can either be classified or unclassified. Critical information that is classified requires OPSEC measures for additional protection because it can be revealed by unclassified indicators. Critical information that is unclassified especially requires OPSEC measures because it is not protected by the requirements provided to classified information. Critical information can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

(5) The term "critical information" is in standard usage with DOD and other Service components.

(6) Essential Elements of Friendly Information (EEFI) are questions about critical information.

(a) The EEFI are questions that the adversary is likely to ask about friendly capabilities, activities, limitations, and intentions (for example, when does the operation begin or where is the operation going to occur?).

(b) The answers to EEFI are critical information.

(c) The use of EEFI protects critical information because it does not reveal sensitive or classified details. Instead of stating the details of critical information, EEFI is critical information converted into a question.

(d) The use of EEFI is an effective way to ensure the widest dissemination of a unit or organization's critical information while protecting classified and sensitive information.

(7) The Critical Information List (CIL) is a consolidated list of a unit or organization's critical information. The CIL will be classified if any one of the items of critical information is classified. At a minimum, the CIL will be sensitive information and must be protected. A method to ensure the widest dissemination of a unit or organization's critical information while protecting it is to convert it to EEFI.

#### *c. Sensitive information.*



(1) Sensitive information (formerly known as sensitive but unclassified (SBU) information) is information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, Department of the Army (DA) civilian, or DOD contractor.

(2) Sensitive information refers to unclassified information and is distinguished from Sensitive Compartmented Information (SCI) which is classified information.

(3) Examples of sensitive information include, but are not limited to:

(a) Unclassified information that requires special handling (for example, Limited Distribution, Encrypt For Transmission Only, and scientific and technical information protected under the Technology Transfer Laws and Arms Export Control Act).

(b) Controlled Unclassified Information (CUI) is unclassified information to which access or distribution limitations have been applied according to national laws, policies, and regulations of the United States Government (U.S. Government). It includes U.S. information that is determined to be exempt from public disclosure according to DODD 5230.25, DODD 5400.7, AR 25-55, AR 340-21, AR 530-1, and so on, or that is subject to export controls according to the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR). Because CUI does not qualify for formal classification, it should be afforded OPSEC measures for additional protection because of its vulnerability as unclassified information.

(c) Information that must be protected under applicable laws such as the Privacy Act (See AR 340-21).

(d) Freedom of Information Act (FOIA)-exempt information specifies nine categories of information that can be withheld from release if requested by the public (See Information Exempt from Release Under the Freedom of Information Act, app L, AR 25-55, and AR 380-5). The category of information that is especially vulnerable is personal information (names, Social Security Numbers, birth dates, and so forth.) Lists of names and accompanying sensitive information of personnel assigned to a unit, organization, or office in the Department of the Army (DA) are prohibited on the World Wide Web. Discretionary release of names and duty information of personnel who frequently interact with the public by nature of their positions and duties-such as general officers and senior executives, PAOs, or other personnel designated as official command spokespersons-is permitted.

(e) Unclassified information designated For Official Use Only (FOUO) is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the FOIA. FOUO is not a classification as FOUO information is unclassified, but is not to be released to the public without undergoing a FOIA and/or legal review. FOUO will be the standard marking for all unclassified products that meet one or more of the exemptions of FOIA, and which if released to the public, could cause harm to Army operations or personnel. Examples include but are not limited to: force protection, movement and readiness data, tactics, techniques, and procedures (TTPs), proprietary information and information protected by copyright, pre-decisional documents, draft publications, and information concerning security systems.

*d. Operations Security (OPSEC) Compromise.*

(1) An OPSEC compromise is the disclosure of critical information or sensitive information which has been identified by the Command and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment.

(2) Critical or sensitive information that has been compromised and is available in open sources and the public domain should not be highlighted or referenced publicly outside of intra-governmental or authorized official communications because these actions provide further unnecessary exposure of the compromised information.

## 1-6. Requirement

a. The National Operations Security (OPSEC) Program (National Security Decision Directive 298) requires each executive department and agency with a national security mission to have an OPSEC program. DODD 5205.02 supports the national program and requires each DOD component to have an OPSEC program.

b. Operations security maintains essential secrecy, which is the condition achieved by the denial of critical information to adversaries. Adversaries in possession of critical information can hinder or prevent friendly mission accomplishment. Thus, essential secrecy is a necessary prerequisite for effective operations. Essential secrecy depends on the combination and full implementation of two approaches to protection:

(1) Traditional security programs to deny adversaries classified information.

(2) Operations security to deny adversaries critical information and indicators of sensitive information.

c. Operations security provides a methodology to manage risk. It is impossible to avoid all risk and protect everything. To attempt complete protection diverts resources from actions needed for mission success.

## 1-7. Application

a. Operations security awareness and execution is crucial to Army success. OPSEC is applicable to all personnel and all Army missions and supporting activities on a daily basis. OPSEC denies adversaries information about friendly capabilities, activities, limitations, and intentions that adversaries need to make competent decisions. Without prior knowledge of friendly actions, adversary leaders cannot act effectively to prevent friendly mission accomplishment. It

applies to all Army activities and is required during training, sustaining, mobilizing, preparing for, and conducting operations, exercises, tests, or activities.

(1) The Army OPSEC program is consistent with joint policy and doctrine in Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3213.01B and Joint Publication 3-13.3. In Joint and Army operations, OPSEC is a core capability of IO as prescribed in JP 3-13.3 and FM 3-13.

(2) Operations security contributes directly to the Army's ability to employ forces superior to an adversary across the full spectrum of operations. Without critical information about our forces, adversaries cannot design and build systems, devise tactics, train, or otherwise prepare their forces (physically or psychologically) in time to effectively counter the Army's capabilities, activities, and intentions, and exploit the Army's limitations.

(3) Combat capability increasingly depends upon maintaining information superiority. This impacts all aspects of raising, equipping, training, deploying, employing and sustaining forces. Every Army organization produces or has information that ultimately affects the ability of U.S. forces to accomplish missions. Every organization must identify and protect this information which an adversary could use against U.S. forces.

(4) Research, development, test, and evaluation (RDT&E) activities are particularly vulnerable to the loss of sensitive information and technology, both classified and unclassified, due to the long life of the development process and the large number of personnel, organizations, and contracted companies involved. Critical information lost during the development process can result in an adversary countermeasure being developed even before a system is fielded. Systems protection, to include the acquisition process, is necessary to preserve the advantage of technological superiority of U.S. forces. OPSEC assessments and surveys will be used to evaluate the vulnerabilities of sensitive information and technology during the research, development, testing, and evaluation phases.

(5) Army Program Executive Officers (PEOs), program managers (PMs), project managers (PMs), and contracting officials must consider OPSEC and incorporate OPSEC implementation as a stipulation in all contracts. All requirements packages must receive an OPSEC review by the user agency (UA) or requiring activity (RA) prior to submission to the Government Contracting Activity (GCA). It is critical that the UA/RA OPSEC Officer identify OPSEC requirements in the scope of work.

(6) The U.S. Government is a party to various arms control agreements, which allow access by foreign officials to U.S. military installations and supporting contractor facilities.

(a) Intermediate-Range Nuclear Forces (INF), Strategic Arms Reduction Treaty (START) and Chemical Weapons Convention (CWC) agreements have provisions for on-site inspections. Under CWC, challenge inspections may occur at sites and in buildings that have nothing to do with declared chemical weapons activity. Regional multi-national treaties such as the Conventional Armed Forces in Europe treaty or the Vienna Document 1999, affect Army units stationed on host country territory. Army units can be subject to observations of unit activity in garrison or while deployed on the territory of a country which is also a treaty participant. With only 72 hours of advance notice, the Open Skies Treaty will allow reconnaissance overflights anytime, anywhere, with few exceptions.

(b) These agreements, while enhancing U.S. national security, provide adversaries with opportunities to collect critical information unrelated to the treaties. Each Army organization or activity must have an OPSEC plan to protect critical information unrelated to legitimate inspection aims. The plan must direct immediate implementation of OPSEC measures for daily vulnerabilities. This may help to avoid compromise of critical information and activities that are likely collateral collection targets of these foreign inspections, unrelated to the treaties. The plan must also have additional measures that are specific for a particular inspection regime. These additional OPSEC measures must be ready for implementation after notice of an impending inspection.

b. Operations security is more important now than it has ever been. The U.S. faces cunning and ruthless adversaries fighting asymmetrically to avoid our strengths. The first step for them to inflict harm is to gather information about us. They are exploiting the openness and freedoms of our society by aggressively reading and collecting material that is needlessly exposed to them. Good OPSEC practices can prevent these compromises and allow us to maintain essential secrecy about our operations.

## 1-8. Proponent

The Deputy Chief of Staff (DCS) G-3/5/7 is the Army's proponent for OPSEC. Subsequently, the command, unit, activity, or installation operations officer is the staff proponent for OPSEC. However, the success or failure of OPSEC is ultimately the responsibility of the Commander and the most important emphasis for implementing OPSEC comes from the chain of command.

a. Operations security is an operations function that protects critical information and requires close integration with other security programs.

b. A unit or organization's Commander, operations officer, and the OPSEC Officer must consider OPSEC in all unit activities to maintain operational effectiveness.

(1) Unit actions are a primary source of indicators collected by adversaries. The Commander, advised by the OPSEC Officer, controls these actions, assigns tasks, and allocates resources to implement OPSEC measures (see app F).

(2) By constantly observing activities, the OPSEC Officer can evaluate these measures for their effectiveness and their impact on operational success.

c. In organizations without a specified operations staff, the element with primary responsibility for planning, coordinating, and executing the organization's mission activities will be the proponent for OPSEC.

d. While the OPSEC Officer is responsible for the development, organization, and administration of an OPSEC program, the Commander's emphasis and support from the chain of command is essential to ensure the proper implementation of an OPSEC program.

## **Chapter 2 Responsibilities**

### **2-1. All Army personnel**

Operations security is everyone's responsibility. Failure to properly implement OPSEC measures can result in serious injury or death to our personnel, damage to weapons systems, equipment and facilities, loss of sensitive technologies and mission failure. OPSEC is a continuous process and an inherent part of military culture and as such, must be fully integrated into the execution of all Army operations and supporting activities. All Department of the Army (DA) personnel (active component, reserve component to include U.S. Army Reserve, Army National Guard, and DA civilians), and DOD contractors will—

a. Know what their organization considers to be critical information, where it is located, who is responsible for it, how to protect it, and why it needs to be protected.

b. Protect from disclosure any critical information and sensitive information to which they have personal access.

(1) Commanders will issue orders, directives, and policies for unit or organization personnel to protect critical and sensitive information in order to clearly define the specific OPSEC measures that all personnel should practice.

(2) A failure to comply with these orders, directives, or policies may be punished as violations of a lawful order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or other actions as applicable.

(3) Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

c. Prevent disclosure of critical and sensitive information in any public domain to include but not limited to the World Wide Web, open source publications, and the media.

(1) Do not publicly disseminate, or publish photographs displaying critical or sensitive information. Examples include but are not limited to Improvised Explosive Device (IED) strikes, battle scenes, casualties, destroyed or damaged equipment, personnel killed in action (KIA), both friendly and adversary, and the protective measures of military facilities.

(2) Do not publicly reference, disseminate, or publish critical or sensitive information that has already been compromised as this provides further unnecessary exposure of the compromised information and may serve to validate it.

d. Implement OPSEC measures as ordered by the Commander, director, or an individual in an equivalent position.

e. Actively encourage others (including family members and family readiness groups (FRGs)) to protect critical and sensitive information.

f. Know who their unit, activity, or installation OPSEC Officer is and contact them for questions, concerns, or recommendations for OPSEC-related topics.

g. Consult with their immediate supervisor and their OPSEC Officer for an OPSEC review prior to publishing or posting information in a public forum.

(1) This includes, but is not limited to letters, resumes, articles for publication, electronic mail (e-mail), Web site postings, web log (blog) postings, discussion in Internet information forums, discussion in Internet message boards or other forms of dissemination or documentation.

(2) Supervisors will advise personnel to ensure that sensitive and critical information is not to be disclosed. Each unit or organization's OPSEC Officer will advise supervisors on means to prevent the disclosure of sensitive and critical information.

h. Process, store, or transmit classified information no higher than the approved accreditation level of a DOD computer system, including all related equipment, networks and network devices (including Internet access) and removable media devices.

(1) DOD computer systems may be monitored for all lawful purposes, to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Network monitoring is done in accordance with AR 25-2 and AR 380-53.

(2) Unauthorized use of a DOD computer system may subject the user to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of a DOD computer system constitutes consent for all lawful purposes.

(3) When an encryption feature is available on unclassified networks, encrypt e-mail messages containing sensitive

information. (See para 1-6c for examples of sensitive information.) Encryption serves as an OPSEC measure to protect sensitive information transmitted over unclassified networks.

i. Consider handling attempts by unauthorized personnel to solicit critical information or sensitive information as a Subversion and Espionage Directed Against the U.S. Army (SAEDA) incident per AR 381-12.

(1) DA personnel who have been involved in or have knowledge of a SAEDA incident will report all facts immediately to the nearest supporting counterintelligence (CI) office as required by AR 381-12.

(2) If these offices are not readily available, SAEDA incidents will be reported to the unit or organization security manager or commander.

(3) Security managers and commanders will ensure that, without exception, reports are relayed as securely and expeditiously as possible, but in all cases within 24 hours, to the nearest CI element.

(4) If counterintelligence support is not available, call the 1-800-CALL-SPY (1-800-225-5779) hotline, leave a message with your name and telephone number and no further details.

j. Destroy (burn, shred, and so forth) critical and sensitive information that is no longer needed to prevent the inadvertent disclosure and reconstruction of this material.

## 2-2. Commanders at all levels

**Note.** *For the purpose of this regulation, this designation applies to all four categories of command: operations, strategic support, recruiting and training, and installation.*

a. Commanders at all levels are responsible for ensuring that their units, activities, or installations plan, integrate, and implement OPSEC measures to protect their command's critical information in every phase of all operations, exercises, tests, or activities.

(1) Commanders at all levels are responsible for issuing orders, directives, and policies to protect their command's critical and sensitive information in order to clearly define the specific OPSEC measures that their personnel should practice.

(2) Personnel who fail to comply with orders, directives, or policies to protect critical and sensitive information may be punished under violations of a lawful order under UCMJ, Art. 92 or under other disciplinary, administrative, or other actions as applicable.

(3) Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

b. Commanders will ensure that their OPSEC program or OPSEC measures are coordinated and synchronized with the higher command's security programs such as information security (INFOSEC), information assurance (IA), physical security, force protection, and so forth.

c. Commanders will ensure all official information released to the public, to include the World Wide Web, receives an OPSEC review prior to dissemination. See paragraph 2-3a (15) for more details.

## 2-3. Commanders of units, activities, and installations at battalion and higher echelons

**Note:** *For the purpose of this regulation, a unit or activity is at battalion level or a higher echelon when its commander or director is a lieutenant colonel (or civilian equivalent) or higher. This applies to any unit or activity authorized by either a modified table of organization and equipment (MTOE) or a table of distribution and allowances (TDA). This section applies to all four categories of command: operations, strategic support, recruiting and training, and installation. Garrison Commands have additional requirements in paragraph 2-23. Program executive officers, product managers, project managers are addressed in paragraph 2-7. The HQDA Staff and Army Command, Army Service Component Command, and Direct Reporting Unit staff organizations are addressed in paragraph 2-4b.*

a. In addition to the requirements outlined in paragraph 2-2, commanders at battalion and higher echelons will develop and implement a functioning, active, and documented (formal) OPSEC program for their unit, activity, or installation to meet their specific needs and to support the OPSEC programs of higher echelons. To develop and implement a formal OPSEC program, commanders will—

(1) Appoint an OPSEC Officer in writing with responsibility for supervising the execution of proper OPSEC within their organization. This appointment may be an additional duty.

(2) Ensure that the appointed OPSEC Officer receives appropriate training in accordance with chapter 4 of this regulation, and that they are of sufficient rank or grade to execute their responsibilities.

(3) Establish a documented OPSEC program that includes as a minimum, OPSEC Officer appointment orders and an OPSEC SOP. At a minimum, the OPSEC standing operating procedure (SOP) should include the unit or activity's critical information and OPSEC measures to protect it.

(4) If assigned intelligence and counterintelligence (CI) capabilities, provide intelligence and CI support to the command's OPSEC program. When this is not practical or possible, forward requirements through channels to the appropriate threat analysis center. The OPSEC process depends on reliable intelligence and CI support to properly identify critical information, analyze the threat, analyze vulnerabilities, conduct a risk assessment, and implement OPSEC measures.

(5) Approve the unit, activity, or installation Critical Information List (CIL) or Essential Elements of Friendly

)  
)  
)  
)  
)  
)  
)  
)

 $\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Enclosure 4**

3 August 2012



Effective: July 15, 2004

United States Code Annotated Currentness

Title 18. Crimes and Criminal Procedure (Refs & Annos)

■ Part I. Crimes (Refs & Annos)

■ Chapter 31. Embezzlement and Theft (Refs & Annos)

➔ § 641. Public money, property or records

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted--

Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case, does not exceed the sum of \$1,000, he shall be fined under this title or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

#### CREDIT(S)

(June 25, 1948, c. 645, 62 Stat. 725; Sept. 13, 1994, Pub.L. 103-322, Title XXXIII, § 330016(1)(H), (L), 108 Stat. 2147; Oct. 11, 1996, Pub.L. 104-294, Title VI, § 606(a), 110 Stat. 3511; July 15, 2004, Pub.L. 108-275, § 4, 118 Stat. 833.)

#### HISTORICAL AND STATUTORY NOTES

##### Revision Notes and Legislative Reports

1948 Acts. Based on Title 18, U.S.C., 1940 ed., §§ 82, 87, 100, 101 (Mar. 4, 1909, c. 321, §§ 35, 36, 47, 48, 35 Stat. 1095, 1096-1098; Oct. 23, 1918, c. 194, 40 Stat. 1015; June 18, 1934, c. 587, 48 Stat. 996; Apr. 4, 1938, c. 69, 52 Stat. 197; Nov. 22, 1943, c. 302, 57 Stat. 591).

) ) ) ) ) ) ) ) )

 $\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Enclosure 5**

3 August 2012

P

Effective: October 11, 1996

United States Code Annotated Currentness

Title 18. Crimes and Criminal Procedure (Refs &amp; Annos)

■ Part I. Crimes (Refs &amp; Annos)

■ Chapter 37. Espionage and Censorship (Refs &amp; Annos)

→ → § 793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument,



appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer--

Shall be fined under this title or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(h)(1) Any person convicted of a violation of this section shall forfeit to the United States, irrespective of any provision of State law, any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, from any foreign government, or any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, as the result of such violation. For the purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse

Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)) shall apply to--

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853(b), (c), and (e)-(p)) shall apply to--

- (A) property subject to forfeiture under this subsection;
- (B) any seizure or disposition of such property; and
- (C) any administrative or judicial proceeding in relation to such property.

if not inconsistent with this subsection.

(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

(4) Notwithstanding section 524(c) of title 28, there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

#### CREDIT(S)

(June 25, 1948, c. 645, 62 Stat. 736; Sept. 23, 1950, c. 1024, Title I, § 18, 64 Stat. 1003; Aug. 27, 1986, Pub.L. 99-399, Title XIII, § 1306(a), 100 Stat. 898; Sept. 13, 1994, Pub.L. 103-322, Title XXXIII, § 330016(1)(L), 108 Stat. 2147; Oct. 14, 1994, Pub.L. 103-359, Title VIII, § 804(b)(1), 108 Stat. 3440; Oct. 11, 1996, Pub.L. 104-294, Title VI, § 607(b), 110 Stat. 3511.)

(June 25, 1948, c. 645, 62 Stat. 736; Sept. 23, 1950, c. 1024, Title I, § 18, 64 Stat. 1003; Aug. 27, 1986, Pub.L. 99-399, Title XIII, § 1306(a), 100 Stat. 898; Sept. 13, 1994, Pub.L. 103-322, Title XXXIII, § 330016(1)(L), 108 Stat. 2147; Oct. 14, 1994, Pub.L. 103-359, Title VIII, § 804(b)(1), 108 Stat. 3440; Oct. 11, 1996, Pub.L. 104-294, Title VI, § 607(b), 110 Stat. 3511.)

#### HISTORICAL AND STATUTORY NOTES

##### Revision Notes and Legislative Reports

1948 Acts. Based on §§ 31 and 36 of Title 50, U.S.C., 1940 ed., War and National Defense (June 15, 1917, c. 30, Title I, §§ 1, 6, 40 Stat. 217, 219; Mar. 28, 1940, c. 72, § 1, 54 Stat. 79).

1948 Acts. Based on §§ 31 and 36 of Title 50, U.S.C., 1940 ed., War and National Defense (June 15, 1917, c. 30, Title I, §§ 1, 6, 40 Stat. 217, 219; Mar. 28, 1940, c. 72, § 1, 54 Stat. 79).

Section consolidated §§ 31 and 36 of Title 50, U.S.C., 1940 ed., War and National Defense.

Section consolidated §§ 31 and 36 of Title 50, U.S.C., 1940 ed., War and National Defense.

) ) ) ) ) ) ) ) ) )

)

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

100

**Enclosure 6**

3 August 2012

▷

Effective: September 26, 2008

United States Code Annotated Currentness

Title 18. Crimes and Criminal Procedure (Refs &amp; Annos)

■ Part I. Crimes (Refs &amp; Annos)

■ Chapter 47. Fraud and False Statements (Refs &amp; Annos)

→ § 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United

States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [FN1]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be

punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that

occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subsection (a) (5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for--

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

[5] Repealed. Pub.L. 110-326, Title II, § 204(a)(2)(D), Sept. 26, 2008, 122 Stat. 3562]

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--



(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, [FN2] with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

- (1) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;
- (5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer’s relationship with the financial institution;
- (6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter;
- (7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
- (8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;
- (9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
- (10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
- (11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
- (12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
- (f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
- (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the

damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section [FN3]

#### CREDIT(S)

(Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub.L. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub.L. 103-322, Title XXIX, § 290001(b) to (f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub.L. 107-56, Title V, § 506(a), Title VIII, § 814, Oct. 26, 2001, 115 Stat. 366, 382; Pub.L. 107-273, Title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub.L. 107-296, Title II, § 225(g), Nov. 25, 2002, 116 Stat. 2158; Pub.L. 110-326, Title II, §§ 203, 204(a), 205 to 208, Sept. 26, 2008, 122 Stat. 3561, 3563.)

)  
 )  
 )  
 )  
 )  
 )  
 )  
 )

**Y.**

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

### Government Motion to Take Judicial Notice

**Enclosure 7**

3 August 2012



# Federal Register

---

Tuesday,  
January 5, 2010

---

## Part VII

## The President

---

Executive Order 13526—Classified  
National Security Information  
Memorandum of December 29, 2009—  
Implementation of the Executive Order  
“Classified National Security Information”  
Order of December 29, 2009—Original  
Classification Authority

---

# Presidential Documents

---

## Title 3—

Executive Order 13526 of December 29, 2009

## The President

## Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**PART 1—ORIGINAL CLASSIFICATION**

**Section 1.1. *Classification Standards.*** (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
  - (2) create any substantive or procedural rights subject to judicial review.
- (c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

**Sec. 1.2. *Classification Levels.*** (a) Information may be classified at one of the following three levels:

- (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the

national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

**Sec. 1.3. Classification Authority.** (a) The authority to classify information originally may be exercised only by:

(1) the President and the Vice President;

(2) agency heads and officials designated by the President; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent

with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information.

**Sec. 1.4. *Classification Categories.*** Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- (h) the development, production, or use of weapons of mass destruction.

**Sec. 1.5. *Duration of Classification.*** (a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or classified information that contains incomplete declassification instructions or lacks declassification instructions shall be declassified in accordance with part 3 of this order.

**Sec. 1.6. *Identification and Markings.*** (a) At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

- (1) one of the three classification levels defined in section 1.2 of this order;
- (2) the identity, by name and position, or by personal identifier, of the original classification authority;
- (3) the agency and office of origin, if not otherwise evident;
- (4) declassification instructions, which shall indicate one of the following:



(A) the date or event for declassification, as prescribed in section 1.5(a);  
(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or

(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant and revoke temporary waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

**Sec. 1.7. *Classification Prohibitions and Limitations.*** (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

- (1) conceal violations of law, inefficiency, or administrative error;
- (2) prevent embarrassment to a person, organization, or agency;
- (3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may not be reclassified after declassification and release to the public under proper authority unless:

(1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;

(2) the information may be reasonably recovered without bringing undue attention to the information;

(3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

**Sec. 1.8. Classification Challenges.** (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

**Sec. 1.9. Fundamental Classification Guidance Review.** (a) Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

## **PART 2—DERIVATIVE CLASSIFICATION**

**Sec. 2.1. Use of Derivative Classification.** (a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

**Sec. 2.2. Classification Guides.** (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.

(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides, provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

(1) information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and

(2) specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

#### **PART 3—DECLASSIFICATION AND DOWNGRADING**

**Sec. 3.1. Authority for Declassification.** (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

(1) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;

(2) the originator's current successor in function, if that individual has original classification authority;

(3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or (4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(e) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

#### **Sec. 3.2. Transferred Records.**

(a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

#### **Sec. 3.3 Automatic Declassification.**

(a) Subject to paragraphs (b)–(d) and (g)–(j) of this section, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(j) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

- (1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign

government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.

(2) The notification shall include:

(A) a description of the file series;

(B) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declassification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.

(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.

(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(B) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.

#### **Sec. 3.4. Systematic Declassification Review.**

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records:

(1) accessioned into the National Archives; (2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

#### **Sec. 3.5. Mandatory Declassification Review.**

(a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:



(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent President's White House Staff or the incumbent Vice President's Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(f) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of National Intelligence shall develop special procedures for the review of information pertaining to intelligence sources, methods, and activities; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

**Sec. 3.6. Processing Requests and Reviews.** Notwithstanding section 4.1(f) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

- (1) the specific information has been approved pursuant to section 3.3(f) of this order for exemption from automatic declassification; and
- (2) the extension does not exceed the date established in section 3.3(f) of this order.

**Sec. 3.7. National Declassification Center.** (a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

- (1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.
- (2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;
- (3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;
- (4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;
- (5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;
- (6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and
- (7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

- (1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and
- (2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt

or declassify information originated by their agency contained in records accessioned into the National Archives, after consultation with subject-matter experts as necessary.

(d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.

(e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that relate to records determined to have permanent historical value.

(f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence, the Director shall also retain such authority with respect to the Intelligence Community.

(g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

#### **PART 4—SAFEGUARDING**

##### **Sec. 4.1. General Restrictions on Access.**

(a) A person may have access to classified information provided that:

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

- (2) the person has signed an approved nondisclosure agreement; and

- (3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:

- (1) prevent access by unauthorized persons;

- (2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

(A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved non-disclosure agreement.

(i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction of the President, or with the consent of the originating agency. For the purposes of this section, "foreign government" includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

#### **Sec. 4.2 Distribution Controls.**

(a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee

may authorize the disclosure of classified information (including information marked pursuant to section 4.1(i)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution mechanism for classified information that it distributes. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

**Sec. 4.3. *Special Access Programs.*** (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations.

(1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director of the Information Security Oversight Office and no more than one other employee of the Information Security Oversight Office or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency head shall brief the National Security Advisor, or a designee, on any or all of the agency's special access programs.

(6) For the purposes of this section, the term "agency head" refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the

Attorney General, and the Director of National Intelligence, or the principal deputy of each.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

**Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel.**

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects;

(2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or

(3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of the national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

**PART 5—IMPLEMENTATION AND REVIEW**

**Sec. 5.1. Program Direction.** (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue such directives as are necessary to implement this order. These directives shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

(1) classification, declassification, and marking principles;

(2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;

(3) agency security education and training programs;

(4) agency self-inspection programs; and

(5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

**Sec. 5.2. Information Security Oversight Office.** (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;
- (4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the National Security Advisor;
- (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
- (7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
- (8) report at least annually to the President on the implementation of this order; and
- (9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

**Sec. 5.3. *Interagency Security Classification Appeals Panel.***

**(a) Establishment and administration.**

(1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.

(2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

(3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.

(4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(6) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(7) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and

(4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the *Federal Register*. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the Federal courts; and

(3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

**Sec. 5.4. General Responsibilities.** Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's



original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;

(5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information be established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.

**Sec. 5.5. Sanctions.** (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

#### **PART 6—GENERAL PROVISIONS**

**Sec. 6.1. Definitions.** For purposes of this order:

(a) "Access" means the ability or opportunity to gain knowledge of classified information.

(b) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) "Authorized holder" of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(f) "Classification" means the act or process by which information is determined to be classified information.

(g) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(h) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(i) "Classified national security information" or "classified information" means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(j) "Compilation" means an aggregation of preexisting unclassified items of information.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(n) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding

a specific subject that may be declassified and the elements that must remain classified.

(o) "Derivative classification" means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(p) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) "Foreign government information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "foreign government information" under the terms of a predecessor order.

(t) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

(u) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a "violation," as defined below.

(v) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

(w) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(x) "Intelligence" includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) "Intelligence activities" means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) "Intelligence Community" means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(bb) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

(cc) "National security" means the national defense or foreign relations of the United States.

(dd) "Need-to-know" means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) "Network" means a system of two or more computers that can exchange data or information.

(ff) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(hh) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ii) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(ll) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(nn) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(rr) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) "U.S. entity" includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) "Weapons of mass destruction" means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

**Sec. 6.2. General Provisions.** (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law

by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. The foregoing is in addition to the specific provisos set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.


(e) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

**Sec. 6.3. *Effective Date.*** This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

**Sec. 6.4. *Publication.*** The Archivist of the United States shall publish this Executive Order in the *Federal Register*.



THE WHITE HOUSE,  
December 29, 2010.

---

Federal Register

Vol. 75, No. 5

Friday, January 8, 2010

---

## Presidential Documents

Title 3—

**The President**

**Executive Order 13526 of December 29, 2009—Classified National Security Information**

*Correction*

In Presidential document E9-31418 beginning on page 707 in the issue of Tuesday, January 5, 2010, make the following correction:

On page 731, the date line below the President's signature should read "December 29, 2009."

[illegible] $\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

### Enclosure 8

3 August 2012



[107th Congress Pub. L. Law 40]  
[From the U.S. Government Printing Office]

[DOC#]  
[DOCID: 1:publ040,107]

[Page 115 STAT. 2241]

Public Law 107-40  
107th Congress

Joint Resolution

To authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States. <NOTE: Sept. 18, 2001 - [S.J. Res. 23]>

Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and  
Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and  
Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and  
Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and  
Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States: Now, therefore, be it

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled, <NOTE: Authorization for Use of Military Force. 50 USC 1541 note.>

SECTION 1. SHORT TITLE.

This joint resolution may be cited as the "Authorization for Use of Military Force".

SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) <NOTE: President.> In General.--That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

(b) War Powers Resolution Requirements.--

(1) Specific statutory authorization.--Consistent with section 8(a)(1) of the War Powers Resolution, the Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 8(b), of

the War Powers Resolution.

[[Page 115 STAT. 225]]

(2) Applicability of other requirements.--Nothing in this resolution supercedes any requirement of the War Powers Resolution.

Approved September 18, 2001.

LEGISLATIVE HISTORY--S.J. Res. 23 (H.J. Res. 64):

---

CONGRESSIONAL RECORD, Vol. 147 (2001):

Sept. 14, considered and passed Senate and House.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 37 (2001):

Sept. 18, Presidential statement.

<all>

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE RESPONSE TO  
GOVERNMENT REQUEST FOR  
JUDICIAL NOTICE**

DATED: 17 August 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, moves this Court to deny the Government's request for judicial notice of the joint resolution dated 18 September 2001 authorizing use of force, also known as Public Law 107-40.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Government has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

FACTS

3. PFC Manning is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, Uniform Code of Military Justice (UCMJ) 10 U.S.C. §§ 892, 904, 934 (2010).

4. The original charges were preferred on 5 July 2010. Those charges were dismissed by the convening authority on 18 March 2011. The current charges were preferred on 1 March 2011. On 16 December through 22 December 2011, these charges were investigated by an Article 32 Investigating Officer. The charges were referred on 3 February 2012.

## WITNESSES/EVIDENCE

5. The Defense does not request any witnesses be produced for this motion.

## LEGAL AUTHORITY AND ARGUMENT

6. The Defense objects to the admission of Enclosure 8 to the Government's motion for Judicial Notice dated 3 August 2012 because it is not relevant under M.R.E. 401 and 402.

7. Pursuant to M.R.E. 401, evidence is relevant when it has "any tendency to make the existence of any fact that is of consequence to the determination of the action ore probable or less probable than it would be without the evidence." M.R.E. 402, meanwhile, establishes "evidence which is not relevant is not admissible."

8. Presumably, the Government requests judicial notice of the joint resolution in order to prove some element of Charge I and its Specification, as Article 104 is referenced in sub-paragraph D of the Government's motion. Article 104 requires the Government to prove that PFC Manning gave intelligence to a certain person, did so by indirect means, the person receiving the intelligence was an enemy and the intelligence information was true, at least in part. *See Military Judge's Benchbook, 3-28-4.*

9. Public Law 107-40 states:

That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

10. Public Law 107-40 is not relevant because it does not make any element of Article 104 more or less likely. Article 104 requires proof that the alleged recipient of intelligence was an enemy at the time of the alleged disclosure, yet Public Law 107-40 gives no insight as to whether any particular person was an enemy. While it may be reasonable to presume that one who is subject to a use of force is an enemy<sup>1</sup>, the law offers no insight as to whether the alleged enemy in *this* case is or was subject to a use of force. Rather, it generically states that those responsible for the terrorist attacks of 11 September 2001 are subject to use of force at the President's discretion. There is no evidence on the record that the recipient of the alleged disclosure in this case falls within the group contemplated by Congress when enacting Public Law 107-40. Absent such evidence, Public Law 107-40 does not make it more or less likely that a given person or entity was an enemy at the time of the alleged disclosure of intelligence.

---

<sup>1</sup> Indeed, an "enemy" may be defined as "any other hostile body that our forces may be opposing." *Military Judge's Benchbook, 3-28-4(d).*

11. The Government's request for judicial notice of Public Law 107-40 should be denied. The law in question does not make it more or less likely that any particular person or group was an enemy at the time PFC Manning allegedly gave intelligence to a certain person and is, thus, not relevant. *M.R.E. 401*. As such, Public Law 107-40 should be excluded at this time. *M.R.E. 402*.

CONCLUSION

15. Based on the above, the Defense requests that the Court deny the Government's motion for judicial notice of Public Law 107-40.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Joshua J. Tooman', with a stylized flourish extending to the right.

JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Prosecution Motion**

**for Preliminary Determination  
of Admissibility of  
MRE 404(b) Evidence**

**3 August 2012**

RELIEF SOUGHT

The Prosecution in the above case respectfully requests that this Court make preliminary determinations on the admissibility of evidence of crimes, wrongs, or acts that are not being used to prove character IAW Military Rule of Evidence (MRE) 404(b) and on the use of evidence to rebut the offer of a pertinent character trait of the Accused IAW MRE 404(a). The Government seeks said preliminary determinations to increase the efficiency of the proceedings and to ensure the trier of fact is only presented admissible evidence. See RCM 916(b)(13), discussion.

BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue, the resolution of which is necessary to decide a motion, shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue, the resolution of which is necessary to decide a motion, shall be on the moving party. RCM 905(c)(2). The United States has the burden of persuasion as the moving party.

FACTS

The Accused is charged with one specification of aiding the enemy, one specification of disorders and neglects to the prejudice of good order and discipline and service discrediting, eight specifications of violations of 18 U.S.C. § 793(e), five specifications of violations of 18 U.S.C. § 641, two specifications of violations of 18 U.S.C. § 1030(a)(1), and five specifications of violating a lawful general regulation, in violation of Articles 104, 134, and 92, Uniform Code of Military Justice (UCMJ). See Charge Sheet.

The Accused attended Advanced Individual Training (AIT) in Fort Huachuca, Arizona from April 2008 to August 2008. See Prosecution Exhibit (PE) 4. His platoon sergeant was SFC Brian Madrid. See Enclosure 1. AIT began with a block of instruction on INFOSEC, which teaches the military analyst how to handle and safeguard classified information. Id. The INFOSEC training block of instruction included training on how to properly mark and handle classified information, the meaning of the various classifications, how to effectively use the internet, the value of the internet in research and collection, and operational security including the enemy's use of the internet. See PE 5.

In June 2008, the Accused received corrective training. See Enclosure 1. SFC Madrid required the Accused to give a presentation to the platoon at formation, present a PowerPoint

presentation to SFC Madrid, and prepare a written product. The corrective training was a result of the Accused posting videos on YouTube where he used "buzzwords" such as top secret, secret, classified, and SCIF, which he was taught not to do. SFC Madrid saw one of the videos on YouTube in which the Accused discussed his work in a "secret SCIF" and his handling of classified information. Enclosure 1.

The presentation to the platoon discussed information security, proper handling of information, a Soldier's obligation to protect and not expose classified material, the possibility that a Soldier's disclosure that he or she has access to classified material may be dangerous to the Soldier, and that enemy forces are trying to collect information on the U.S. Military. Id. The written product defined secret information and identified the type of people who try to collect information for use against the United States, such as foreign governments, enemies, spies, hackers, etc. Id. The PowerPoint presentation closely mirrored the written product. Id. The PowerPoint presentation was found on the Accused's external hard drive. See Enclosure 2.

In approximately March 2009, SPC Jihreah Showman became the Accused's supervisor at Fort Drum, New York. Enclosure 3. Both she and the Accused were assigned the MOS 35F and attended training together at the unit, including JRTC training. Id. They also deployed together in October 2009. Id. Before the deployment, SPC Showman counseled the Accused on his military bearing. Id. During this counseling, SPC Showman asked the Accused what the flag meant to him. Id. The Accused responded that the flag meant absolutely nothing to him, and he had no allegiance to the United States or its people. Id. SPC Showman repeated the Accused's statement in a sworn statement given during the investigation into the Accused's misconduct. See Enclosure 4.

On 8 May 2010, the Accused punched SPC Jihreah Showman in the face. See Enclosure 5. Because of this misconduct, the Accused was removed from the 2-10 Mountain SCIF and assigned to work in the supply room. Enclosure 6. He also received an Article 15 for his misconduct. See Enclosure 5.

The prosecution provided the defense MRE 404(b) notice on 6 April 2012. Enclosure 7.

The prosecution published its witness list on 22 June 2012 and named both Ms. Jihreah Showman (SPC Showman) and SFC(R) Brian Madrid as witnesses. See Appellate Exhibit (AE) CLXII.

#### WITNESSES/EVIDENCE

The prosecution requests the Court consider the charge sheet and the 7 listed enclosures.

#### LEGAL AUTHORITY AND ARGUMENT

##### **I. EVIDENCE OF THE ACCUSED'S OTHER WRONGS IS ADMISSIBLE FOR A NONCHARACTER PURPOSE**

In general, MRE 404(a) prohibits admission of evidence of a person's character to prove

action in conformity therewith on a particular occasion. MRE 404(b), however, allows the introduction of evidence of other crimes, wrongs, or acts provided they are not used to show action in conformity with that character on a specific occasion. The prosecution may offer this non-propensity evidence against the Accused in its case in chief as proof of "motive, opportunity, intent, preparation, plan, knowledge, identity or absence of mistake or accident." United States v. Morrison, 52 M.J. 117, 121 (C.A.A.F. 1999) (citing MRE 404(b)). Evidence does not, however, need to fall within one of the nonpropensity examples given by MRE 404(b) to be admissible. United States v. Castillo, 29 M.J. 145, 150 (CMA 1989).

MRE 404(b) "is a rule of inclusion, not exclusion." United States v. Diaz, 59 M.J. 79, 93-94 (C.A.A.F. 2003); see also United States v. Tyndale, 56 M.J. 209, 212 (C.A.A.F. 2001); United States v. Browning, 54 M.J. 1, 6 (C.A.A.F. 2000). MRE 404(b) only excludes propensity evidence, and then goes on to give a nonexhaustive list of the purposes for which the evidence could be admissible. United States v. Johnson, 49 M.J. 467, 473 (C.A.A.F. 1998). "[T]he sole test under Mil.R.Evid. 404(b) is whether the evidence of the misconduct is offered for some purpose other than to demonstrate the Accused's predisposition to crime and thereby to suggest that the fact finder infer that he is guilty . . . ." Castillo, 29 M.J. at 150; see also Huddleston v. United States, 485 U.S. 681, 686 (1988).

To ensure the evidence has a proper purpose under MRE 104(b), 402, and 403, the U.S. Court of Appeals for the Armed Forces (CAAF) applies the following three-pronged test to determine the admissibility of other acts evidence under MRE 404(b): (1) Does the evidence reasonably support a finding by the fact finder that the Accused committed prior crimes, wrongs, or acts? (2) What fact of consequence is made more or less probable by the existence of this evidence? (3) Does the probative value substantially outweigh any potential unfair prejudice? Diaz, 59 M.J. at 94 (citing United States v. Reynolds, 29 M.J. 105, 109 (CMA 1989)). If the evidence meets each of these three tests, it is admissible. Id.

#### **A. The Evidence Reasonably Supports a Finding by the Fact Finder that the Accused Committed Prior Bad Acts**

Whether the evidence reasonably supports a finding that the Accused committed prior crimes, wrongs, or acts, "is founded on [MRE] 104(b) dealing with relevance conditioned on fact." United States v. Acton, 38 M.J. 330, 333 (1994). The Court of Appeals has held that "[t]he threshold for this [first] prong of admissibility is low." Acton, 38 M.J. at 333; see also Browning, 54 M.J. at 6. Acton provides:

[i]n determining whether the Government has introduced sufficient evidence to meet Rule 104(b), the trial court neither weighs credibility nor makes a finding that the Government has proved the conditional fact by a preponderance of the evidence. The court simply examines all the evidence in the case and decides *whether the jury could reasonably find the conditional fact . . . by a preponderance of the evidence.*



38 M.J. at 333 (citing Huddleston, 485 U.S. at 690) (emphasis added); see also Castillo, 29 M.J. at 151 (“[T]he military judge must admit the evidence if he concludes that the fact finder could reasonably find by a preponderance of the evidence that the other misconduct had occurred, even though the judge himself would not make such a finding.”)

All three government witnesses (Ms. Showman, SFC(R) Madrid, and SSG Bigelow) testified under oath at the Article 32. In addition, Ms. Showman gave a sworn statement consistent with her Article 32 testimony regarding the Accused's disloyal statement. The government will offer the slideshow to support SFC(R) Madrid's statement, which was recovered from the Accused's external hard drive. The Accused's actions of punching then-SPC Showman in the face is supported by the Article 15 the Accused received and its supporting documentation. Based on sworn testimony alone, the trier of fact could reasonably find that the Accused committed the misconduct in all instances.

All three witnesses are on the prosecution's witness list. Assuming the above evidence is again elicited under oath at trial, there is sufficient evidence to admit the uncharged misconduct subject to the introduction of the evidence at trial. Accordingly, the first prong of the Reynolds test is conditionally satisfied.

#### **B. The Existence of this Evidence Makes Facts of Consequence More Probable**

MRE 401 defines “relevant evidence” as “evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.” MRE 401. In general, all relevant evidence is admissible. See MRE 402.

The Accused's infractions will directly assist the fact finder in deciding whether or not the Accused had the requisite knowledge to commit the misconduct. The evidence is not being offered to prove character. The training that the Accused presented to his platoon sergeant and his AIT class in response to his breach of INFOSEC/OPSEC shows that the Accused knew that information posted on the internet is accessible to and sought out by the enemy. See Charge Sheet, Charge II, Specification 1; see also Castillo, 29 M.J. at 151 (allowing the fact finder to consider uncharged misconduct between the Appellant and the victim to understand the significance of a gesture). Without discussing the underlying uncharged act, the fact finder will not be able to sufficiently comprehend why the Accused had to complete the various corrective training assignments.

The Accused's disloyal statement to SPC Showman is evidence relevant to the Accused's state of mind. The evidence is not being offered to prove the character of the Accused nor is it being offered to prove motive. The evidence is being offered to show that the Accused made a statement that he had no particular loyalty to the country whose information it was his job to safeguard. The statement is evidence of the Accused's intent for the charged misconduct because it makes it more likely that the Accused did not care if the enemy had access to the information that was posted on the Internet. Specifically, it is circumstantial evidence that the Accused knowingly gave intelligence to the enemy in support of Charge I, Specification 1; that the Accused wrongfully and wantonly caused the information to be published on the internet with

knowledge that it would be accessible to the enemy in support of Charge II, Specification 1; that the Accused's conduct was willful in support of Charge II, Specifications 2, 3, 5, 7, 9, 10, 11, 12, 13, and 15; and that the Accused stole, purloined, or knowingly converted a thing of value to the United States in support of Charge II, Specifications 4, 6, 8, 12, and 16. See Charge Sheet; see, e.g., Huddleston, 485 U.S. at 685 ("Extrinsic acts evidence may be critical to the establishment of the trust as to a disputed issue, especially when that issue involves the actor's state of mind . . ."); United States v. Humphreys, 57 M.J. 83, 91 (C.A.A.F. 2002) (Evidence of "other acts" of the Accused's inappropriate comments was admissible to show Accused's non-innocent intent in making charge inappropriate comment.)

The Accused's misconduct of punching SPC Showman is necessary to show the timeline of the Accused's removal from the SCIF and placement in the Supply Room to work with SSG Bigelow where the Accused's misconduct continued. Because of the battery, the Accused was removed from the 2-10 Mountain SCIF and assigned to work in the supply room. In the supply room, the Accused stole or converted the United States Forces-Iraq (USF-1) Global Address List (GAL). See Charge Sheet, Charge II, Specification 16. Without discussing the underlying misconduct, the sudden change in the Accused's position will be confusing to the panel and the timeline will be unclear. See Castillo, 29 M.J. at 150 ("It is unnecessary . . . that relevant evidence fit snugly into a pigeon hole provided by [MRE] 404(b).")

The uncharged misconduct makes facts of consequence more probable under the liberal admissibility standard outlined in MRE 402. The evidence is not being used to establish character, but is being used to show knowledge, state of mind, and a timeline of events. As such, the information will assist the fact finder in a proper determination on the merits, and satisfies the second prong of the Reynolds analysis.

### **C. The Probative Value Substantially Outweighs any Potential Unfair Prejudice**

Prejudice alone is not sufficient to warrant exclusion. Evidence of a legal relevance theory should only be excluded when the probative value is "substantially outweighed" by the accompanying prejudicial dangers. United States v. Teeter, 12 M.J. 716 (A.C.M.R. 1981) (stating that striking a balance between probative value and prejudicial effect is left to the trial judge and that the balance "should be struck in favor of admission"). Virtually all evidence is prejudicial to one party or another. To justify exclusion the prejudice must be unfair. United States v. Candelaria-Silva, 162 F.3d 698, 705 (1st Cir. 1998). However, "[a]n Accused is not immunized . . . against the Government's use of evidence of other misconduct because the other misconduct was especially flagrant and repugnant." Castillo, 29 M.J. at 151; see also United States v. Stokes, 12 M.J. 229, 239 (1982).

Relevant evidence must be weighed against its tendency to create *unfair* prejudice, mislead the fact finder, cause undue delay, or waste time. United States v. Dimberio, 56 M.J. 20, 24 (C.A.A.F. 2001) (emphasis added). Unfair prejudice occurs when the proffered evidence causes, or leads, the fact finder to make a decision on an improper basis. Old Chief v. United States, 519 U.S. 172, 180 (1997).

Although there is not a clear test to follow, CAAF has stated that factors for military judges to consider in conducting a balancing test are the following:

the strength of the proof of the prior act; the probative weight of the evidence; the potential to present less prejudicial evidence; the possible distraction of the factfinder; the time needed to prove the prior conduct; the temporal proximity of the prior event; the frequency of the acts; the presence of any intervening circumstances; and the relationship between the parties.

United States v. Berry, 61 M.J. 91 (C.A.A.F. 2005) (citing United States v. Wright, 53 M.J. 476, 482 (C.A.A.F. 2000)).

The Accused's INFOSEC/OPSEC breaches at AIT stand up to the factors in Berry. There is strong proof that the Accused committed the misconduct. His platoon sergeant saw and testified under oath to seeing the video posted on YouTube. In addition, CID recovered a corrective training PowerPoint from the Accused's external hard drive that corresponded to the date and content of the PowerPoint that the Accused presented to SFC(R) Madrid. The evidence is probative to the elements concerning the Accused's intent when he compromised information. In particular, the evidence directly establishes the Accused's knowledge required in Charge II, Specification 1. The evidence is also not particularly prejudicial to the Accused, apart from proving his knowledge, especially in light of the charged misconduct. The uncharged act shows a security infraction in a training environment. As stated, the misconduct is being used to elicit sufficient facts for the fact finder to understand the evidence on corrective training, thus minimal time will be spent on those cursory facts. The charged and uncharged misconduct are also temporally proximate as they occurred approximately eighteen months apart—one while the Accused was being trained in his MOS and one while the Accused was working in his MOS. The AIT misconduct occurred in June 2008 and the charged misconduct begins on or about 1 November 2009. The AIT misconduct was limited; however, the charged misconduct ranged over several months, not to mention several databases. There was no presence of intervening circumstances. The Accused committed the misconduct, it was reported by his peers, and it was dealt with by his supervisor. The acts complete a chronological and logical story; removing the acts would create confusing gaps.

SPC Showman's testimony regarding the Accused's disloyal statement also stands up to the factors in Berry. Consistent with her Article 32 testimony, SPC Showman gave a sworn statement reporting the same misconduct by the Accused. The statement will likely be prejudicial to a panel of Soldiers; however, compared to the charged misconduct, the statement is not overly prejudicial when viewed in light of the probative value it has into the Accused's state of mind. All evidence presented to the fact finder regarding the Accused's serious misconduct will be prejudicial to the fact finder. Given the charged misconduct, however, the statement will likely not be a distraction to the fact finder who will be more focused on the serious misconduct charged. The testimony will take minimal time to elicit. The uncharged misconduct occurred in the months immediately preceding the unit's deployment, which is when, on or about November 2009, the charged misconduct began. The statement occurred during one counseling session; however, the charged misconduct ranged over several months, not to mention several databases.

There were no intervening circumstances; the Accused was in a counseling session with a superior, not in a casual setting with a friend.

The Accused's battery of SPC Showman also stands up to the factors in Berry. The act was witnessed by several individuals and testified about under oath at the Article 32 by SPC Showman and others. The battery is relevant to show the circumstances of the Accused's removal from the SCIF and the corresponding timelines of the charged misconduct. There is no less prejudicial evidence to sufficiently explain the Accused's movement to the fact finder. Compared to the charged misconduct, the battery will offer little, if any, distraction for the fact finder. The time needed to show the uncharged misconduct will be very minimal. The uncharged misconduct occurred during the charged misconduct. The specific battery only occurred on one occasion; however, the charged misconduct ranged over several months, not to mention several databases. There was an intervening circumstance of a verbal disagreement between SPC Showman and the Accused; however, that can also be elicited in testimony. The relationship between the parties varied between a superior-subordinate and peers; they were not friends.

In addition to withstanding the factors recommended in Berry, the defense will have ample opportunity at trial, through cross-examination and argument, to attack this evidence's meaning, importance, and weight. Furthermore, the Court can and should issue a limiting instruction to the panel that specifically discusses the permissible and impermissible uses of this evidence. These aspects of trial procedure will help to ensure that the evidence is used only for its proper aforementioned purpose.

Because the probative value of the evidence is not substantially outweighed by the danger of unfair prejudice, the third Reynolds prong is satisfied in this case.

## **II. THE INFOSEC/OPSEC VIOLATIONS, DISLOYAL STATEMENTS, AND BATTERY OF SPC SHOWMAN ARE ADMISSIBLE UNDER M.R.E. 404(A)(1) TO IMPEACH DEFENSE WITNESSES ON GOOD SOLDIER EVIDENCE.**

Evidence of a person's character or a trait of character is generally not admissible for the purpose of proving action in conformity therewith on a particular occasion. MRE 404(a)(1). Evidence of a pertinent trait of character offered by an Accused, or by the prosecution to rebut the same, however, is admissible. Id. "The price a defendant must pay for attempting to prove his good name is to throw open the entire subject which the law has kept closed for his benefit and to make himself vulnerable where the law otherwise shields him." Michelson v. United States, 335 U.S. 469, 479 (1948); see also United States v. Johnson, 46 M.J. 8 (C.A.A.F. 1997).

If a defense witness offers opinion or reputation evidence that the Accused is a good Soldier, the prosecution can rebut that evidence. MRE 404(a)(1). On cross-examination, the Government may inquire into relevant specific instances of the Accused's conduct. MRE 405(a). The questions would refer to the relevant uncharged misconduct, such as the Accused's breach of INFOSEC/OPSEC at AIT, disloyal statements, and battery of SPC Showman. Specifically, the prosecution will test the foundation of the witness's opinion or reputation evidence by asking

"have you heard" or "did you know" questions of that witness. See, e.g., United States v. Pearce, 27 M.J. 121, 124 (C.A.A.F. 1988).

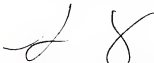
Based on the testimony of the witnesses at the Article 32, the sworn statement, the PowerPoint, the Article 15, and, presumably, the testimony the witnesses will give at trial, the Government has a good faith belief that the Accused did commit all the above discussed misconduct. Id.

The evidence is extremely probative into whether or not the Accused is a good Soldier. Good Soldiers do not breach the security of the information that they were trained to protect, they are loyal to the United States, and they do not punch their peers or superiors in the face. While certainly prejudicial to the defense, the evidence is not unfairly prejudicial such that it would be prohibited by MRE 403.

In addition, the defense will have ample opportunity to argue to the panel their theory of the case. Finally, if the defense believes the evidence is inordinately damaging to their case, they can choose not to call good Soldier witnesses. The risk of prejudice is "a risk undertaken by the defense in electing to present affirmative character evidence." Pearce, 27 M.J. at 125.

### CONCLUSION

The prosecution requests the Court grant the prosecution's motion and preliminarily determine the uncharged acts are admissible pursuant to MRE 104(b), 402, 403, and 404(b), as all three Reynolds prongs are satisfied, and that the evidence is admissible for a different purpose under MRE 404(a)(1) if the defense presents good Soldier evidence.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

I certify that I have served or caused to be served a true copy of the above on the Defense counsel on 3 August 2012.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

7 Encls

1. Summarized Article 32 Testimony, SFC Madrid

2. Accused's PowerPoint Presentation, 13 Jun 08
3. Summarized Article 32 Testimony, SPC Showman
4. Sworn Statement, SPC Showman
5. Article 15 Packet
6. Summarized Article 32 Testimony, SSG Bigelow
7. MRE 404(b) Notice, 6 Apr 11

) ) ) ) ) ) ) ) )

**Y.**

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Prosecution Motion  
for Preliminary Determination  
of Admissibility of  
MRE 404(b) Evidence**

**Enclosure 1**

**3 August 2012**

BRIAN MADRID, Civilian, was called as a witness for the government, was sworn, and testified in substance as follows:

DIRECT EXAMINATION

Questions by Assistant Trial Counsel 2:

I retired in the middle of September 2010; I served in the Army for 22 years. I was a 35T, which is a Electronic Warfare Military Intelligence System Integrator and Maintainer. I worked on all of the MI collection systems, computers networks, communications equipment, and we were also evolving into the exploitation of captured enemy equipment such as PDA, laptops, and phones. I was PFC Manning's AIT Platoon Sergeant; he attended advanced individual training at Fort Huachuca. He attended training there, I believe, from April until August 2008. I was in the Platoon Sergeant position from between February 2008 until August 2010; that's about 2 1/2 years.



1 PFC Manning is a 35F, a Military Intelligence Analyst. I  
2 am familiar with the 35F block of instruction. The first block  
3 of instructions that they received I believe it is called,  
4 "INFOSEC," and it is basically instructing the military analyst  
5 how to handle and the safeguarding of classified information. I  
6 know that is the first block of instruction because I would talk  
7 to the instructors, and students would always come back and say  
8 how much they enjoyed the class. In order to attend that AIT  
9 they have to have an interim TS/SCI security clearance. The  
10 accused was required to do corrective training in AIT. I believe  
11 that was in June 2008. Some Soldiers had come to me one  
12 afternoon explaining that Private Manning had been posting  
13 videos on YouTube, and he was using words such as top secret,  
14 secret, classified, and SCIF which he was taught not to do.  
15 Allegedly, there were three videos; because of the limitations  
16 with our local network, we had YouTube blocked, so we had one of  
17 the Soldier's laptop and used the wireless Internet to see one  
18 of the videos. The video was of him inside of his barracks room  
19 speaking about his daily life; then he began to branch off onto  
20 subjects like well I work at this secret SCIF, I handled this  
21 classified information, using buzzwords like that. The  
22 corrective training at the time that he was required to do a  
23 presentation to the company, and whenever we had the Soldiers do  
24 that type of corrective training, he would have presented it to  
25 us first to ensure that the Soldiers were going to present an  
26 informative product. I also had him present me with a type  
27 memorandum stating that he basically understood that he wasn't  
28 supposed to do that type of thing. He wasn't supposed to expose  
29 himself, a person with clearance with access to that type of  
30 information. The presentation in front of the unit was about  
31 information security, how to handle it, and especially if you  
32 are a person with access to this type of material you are not to  
33 expose the material or that you have access to it. And that it  
34 can be dangerous to personnel that are in the military and that  
35 there are people, enemy forces that are trying to collect  
36 information on the US military. The substance of the type  
37 product was basically what secret information is, the type of  
38 people that are trying to collect against the government such  
39 as, foreign governments, enemies, spies, hackers, items like  
40 that. The PowerPoint was very similar to the written product  
41 but it had more reference to regulations. He did three total  
42 types of corrective training-the presentation in front of the  
43 platoon, the PowerPoint, and the memorandum.

#### 44 CROSS-EXAMINATION

45  
46 Questions by the civilian defense counsel:  
47

1  
2 The AIT course Intel analyst is 16 weeks and 3 days. And  
3 part of the AIT instruction is done in the classroom, and part  
4 of that instruction is done in the field. Me being a platoon  
5 Sergeant I had anywhere from 140 to 150 Soldiers. I do get to  
6 know an occasional Soldier depending upon the situation, there  
7 are some Soldiers that you have to dedicate a lot of your time  
8 to, and then there are some Soldiers that are really low  
9 maintenance. I generally get to know most of them. It would be  
10 a fair assessment to say that I do not get to know them all very  
11 well. The training that they received consisted of a lot of  
12 training, there is a lot of training compacted. I don't think  
13 that is unreasonable to say that it is firehose mentality. This  
14 is the initial course for someone being trained as a military  
15 intelligence analyst. At the end the AIT students conduct a  
16 ten-day field exercise. Once they complete that then they  
17 graduate and go on to their first duty assignment. Once they  
18 graduate they have a basic understanding they are by no means an  
19 expert in that field. The expertise for the Intel analyst comes  
20 as they learn on-the-job training through time. After I watched  
21 that video I showed to Captain Ogletree, the video did not  
22 discuss any specific operational security, but he was using the  
23 buzzwords top secret, classified, words of that nature. This  
24 video was intended for friends and family, that was the target  
25 audience. I do not recall him saying anything about him missing  
26 his family but I do recall him talking about barracks life in  
27 the video. Those buzzwords in and of themselves are not  
28 classified, they are pretty well known. Just referencing those  
29 words in the video is not a security breach because it  
30 referenced those words and he was an AIT student he had to do  
31 some sort of corrective training. I personally do not have any  
32 ability to suspend his clearance, even though he was counseled  
33 for this incident he did not lose his security clearance over  
34 it, had it been suspended he would not have been able to  
35 complete his training.

#### 36 37 REDIRECT EXAMINATION

#### 38 39 Questions by Assistant Trial Counsel 2:

40  
41 Those Soldiers are taught not to use those buzzwords  
42 because if they were to identify themselves to outside personnel  
43 they give themselves an element of possible compromise.  
44 Somebody on the outside could find out that they had a security  
45 clearance, they could target the individual because they have  
46 access to a certain level of information.  
47

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34

**OBJECTION**

The defense counsel objected and asked the Investigating Officer to voir dire the witness.

The Investigating Officer granted the defense counsel's request.

**VOIR DIRE**

I am not a 35F trainer. I was an AIT platoon Sergeant who was in charge of those students. I had nothing to do with the setting up of classes, but I sat through a class. I did not do any of the instruction for those students.

The defense counsel objected stating that this witness was not an expert in the training of the AIT students.

The Investigating Officer instructed the trial counsel to lay a proper foundation before asking those types of questions.

**The redirect examination by Assistant Trial Counsel 2 continued as follows:**

I did not sit through all of the classes that the students attended but I sat through about 3 or 4 classes for each block, and the length of each block varied. I did sit through the first portion of instruction which discusses classified information. And in that first block of instruction they stated that you can't transmit classified permission to someone who is not authorized to have it.

[The witness was permanently excused, duly warned, and ended the call.]

)
)
)
)
)
)
)
)
)

 $\gamma_{\alpha}$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Prosecution Motion  
for Preliminary Determination  
of Admissibility of  
MRE 404(b) Evidence**

**Enclosure 2**

**3 August 2012**

UNCLASSIFIE

D

# *Operations Security (OPSEC)*

PV2 Manning, Bradley

D Company, 305<sup>th</sup> Military Intelligence Battalion

Friday, 13 Jun 08

UNCLASSIFIE

D

UNCLASSIFIED

D

## *Executive Summary*

- Definition of OPSEC
- Types of OPSEC Information
- Common OPSEC Violations
- Protection from Adversaries
- Conclusion

UNCLASSIFIED

D

UNCLASSIFIED

D

## *Definition of OPSEC*

- Operations Security (OPSEC)
- Protection of Information:
  - Public Assets
  - Military Assets
  - Personnel
  - Families of Personnel
  - National Security

UNCLASSIFIED

D

## INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

**USE OF FORM** - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

**COPIES** - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

**ARRANGEMENT** - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.
2. Judge advocate's review pursuant to Article 64(a), if any.
3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.
4. Briefs of counsel submitted after trial, if any (Article 38(c)).
5. DD Form 494, "Court-Martial Data Sheet."
6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.
7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

- a. Errata sheet, if any.
- b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.
- c. Record of proceedings in court, including Article 39(a) sessions, if any.
- d. Authentication sheet, followed by certificate of correction, if any.
- e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.
- f. Exhibits admitted in evidence.
- g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.
- h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.